Towers of Function Fields over Cubic Fields

Dissertation
zur Erlangung des Grades
Doktor der Naturwissenschaften
(Dr. rer. nat.)

vorgelegt beim
Fachbereich Mathematik
der Universität Duisburg-Essen

von **Alp Bassa**
aus Offenbach am Main

November 2006

Tag der Disputation	07.02.2007
Vorsitzender:	Prof. Dr. Norbert Weck
Gutachter:	Prof. Dr. Dr. h.c. Gerhard Frey
	Prof. Dr. Henning Stichtenoth

Acknowledgments

First and foremost, I would like to express my deepest gratitude to my "Doktorvater", Henning Stichtenoth, without whom this thesis would not have been possible.

I am honored to have Gerhard Frey as a member of my committee. I would like to express my sincere gratitude to him for his continuous support.

It is a pleasure to thank Peter Beelen, Irene Bouw and Arnaldo Garcia for fruitful discussions, for their encouragement and for all their help.

I also wish to thank the members of the Department of Mathematics at the University of Duisburg-Essen, the Institute for Experimental Mathematics and the Sabancı University for the friendly atmosphere and the stimulating working environment.

Sincere appreciation is due to Mehpare Bilhan and Özgür Kişisel for introducing me to this topic and for their guidance and constant support during my undergraduate studies.

I would like to thank the Graduiertenkolleg "Mathematische und ingenieurwissenschaftliche Methoden für sichere Datenübertragung und Informationsvermittlung" (DFG) for the generous funding and for providing such a vivacious working atmosphere.

Last but not least, I thank my family, whose love and support have accompanied me throughout my life.

Introduction

Let F be an algebraic function field of one variable with the finite field $\mathbb{F}_\ell$ as its full field of constants. Let g be the genus of F and denote by $N(F)$ the number of $\mathbb{F}_\ell$-rational places of F. The Hasse–Weil bound gives an upper bound for $N(F)$ in terms of g and ℓ. This bound is not optimal, when the genus is large compared to the cardinality of the finite field, see [9, 13]. To study the asymptotic behaviour with increasing genus, let $N_\ell(g)$ be the maximal number of $\mathbb{F}_\ell$-rational places that a function field over $\mathbb{F}_\ell$ of genus g can have. It was shown by Drinfel'd and Vlăduţ [3], that

$$A(\ell) := \limsup_{g\to\infty} \frac{N_\ell(g)}{g} \leq \sqrt{\ell} - 1.$$

If ℓ is a square (an even power of a prime), then the above inequality is in fact an equality; i.e., $A(\ell) = \sqrt{\ell} - 1$, see [9, 22].

If ℓ is not a square, not much is known about the exact value of $A(\ell)$. Using class field towers, Serre [17, 18] showed that there exists a constant $c > 0$, which is independent of ℓ, such that $A(\ell) \geq c \cdot \log \ell > 0$ for all ℓ.

Using degenerations of Shimura modular surfaces, Zink [24] showed that

$$A(p^3) \geq \frac{2(p^2-1)}{p+2},$$

if p is a prime number.

In [8], van der Geer and van der Vlugt gave an *explicit* example of a tower $\mathcal{E} = (E_n)_{n\geq 0}$ over the finite field with eight elements, with limit

$$\lambda(\mathcal{E}) := \lim_{n\to\infty} \frac{N(E_n)}{g(E_n)} = \frac{3}{2},$$

which attains Zink's lower bound for $p = 2$. Their tower is given as follows: $E_0 = \mathbb{F}_8(x_0)$ and $E_{i+1} = E_i(x_{i+1})$ for $i \geq 0$, where

$$x_{i+1}^2 + x_{i+1} = x_i + 1 + 1/x_i. \tag{0.1}$$

Zink's lower bound was generalized by Bezerra, Garcia and Stichtenoth [2] to arbitrary cubic finite fields. This was done by providing an explicit tower of function fields $\mathcal{F} = (F_n)_{n\geq 0}$ over the finite field $\mathbb{F}_\ell$, where $\ell = q^3$ for an arbitrary prime power q, with limit

$$\lambda(\mathcal{F}) = \lim_{n\to\infty} \frac{N(F_n)}{g(F_n)} \geq \frac{2(q^2-1)}{q+2}. \tag{0.2}$$

This tower is recursively given as follows:[1] $F_0 = \mathbb{F}_\ell(x_0)$ and $F_{i+1} = F_i(x_{i+1})$ for $i \geq 0$, where

$$x_{i+1}^q - x_{i+1}^{q-1} = 1 - x_i + \frac{1}{x_i^{q-1}} \tag{0.3}$$

We call the tower $\mathcal{F}$, which is defined by Equation (0.3) the Bezerra–Garcia–Stichtenoth tower (BGS tower for short). The case $q = 2$ corresponds to the van der Geer–van der Vlugt tower, see Equation (0.1). The case $q > 2$ is substantially different. In this case the extensions F_{i+1}/F_i $(i \geq 0)$ are not even Galois. The BGS tower (the van der Geer–van der Vlugt tower for $q = 2$) is the only known example of an explicit tower over a nonsquare field with such a large limit.

The main aim of this thesis is to give a simpler and more transparent proof for the limit of the BGS tower.

In Section 1, we recall shortly basic definitions and properties of towers and introduce some notation.

In Section 2 we start by proving some basic facts about the BGS tower. The proof of Inequality (0.2) splits naturally into two problems:

(i) to give a *lower* bound for the numbers $N(F_n)$;

(ii) to give an *upper* bound for the genus $g(F_n)$, for all $n \geq 0$.

The first problem is relatively easy: one shows that sufficiently many rational places of the field F_0 split completely in all extensions F_n/F_0. In Section 2 we give a simpler proof of this fact than the proof given in [2], see Theorem 2.6. This is done by providing a functional equation, which shows in a more natural way, why the given places split completely in all extensions. In this section we also introduce the pyramid corresponding to the tower and point out the main difficulties in determining the limit of the BGS tower.

The hard part in proving Inequality (0.2) is the second problem, namely to give upper bounds for the genus $g(F_n)$, for all $n \geq 0$. Here one has to find an upper bound for the degree of the differents in the extensions F_n/F_0. Since there occurs wild (and in the case $q \neq 2$ also tame) ramification in F_n/F_0, the precise determination of different degrees requires careful and long calculations. The original proof of Inequality (0.2) given by Bezerra, Garcia and Stichtenoth is rather long and very technical, cf. [2, Sec. 4]. In Section 3 we replace the complex calculations in their work by structural arguments, thus giving a much simpler, shorter and more transparent proof for the limit of the BGS tower.

These arguments are of course not just developed to be used to simplify the proof of the BGS tower, they also apply to other towers. So we use them for instance in Section 4 to compute the limit of the Galois closure of the BGS tower. The Galois closure of the BGS tower is again a tower over $\mathbb{F}_\ell$, where $\ell = q^3$. We show that the limit $\lambda(\mathcal{E})$ of the Galois closure $\mathcal{E}$ satisfies

$$\lambda(\mathcal{E}) \geq \frac{2(q^2-1)}{q+2}.$$

[1] the presentation of this tower in [2] is slightly different, see Section 2 below

Note that this bound for the limit of the Galois closure coincides with the bound given by Inequality (0.2) for the limit of the tower itself.

One of the main tools used while determining the limit of the BGS tower and of its Galois closure is a lemma from ramification theory. This "key lemma" was proved in [4] in the case of function fields. In Section 5 we give a proof of this result using the theory of higher ramification groups, which is valid for more general fields.

It was shown in [21], that several classes of codes over finite fields with square cardinality, including the class of transitive codes and the class of self-dual codes, attain the Tsfasman–Vlăduţ–Zink bound. In Section 6, the same problem is considered over cubic finite fields. Starting from the BGS tower, a new Galois tower $\mathcal{E}'$ is constructed, which has the same limit as the BGS tower. The notion of r-quasi transitive codes is introduced (in analogy to quasi-cyclic codes), and, using the tower $\mathcal{E}'$, asymptotic lower bounds are obtained for the class of r-quasi transitive codes over cubic finite fields. Also, using this tower, asymptotic lower bounds are obtained for the class of transitive isoorthogonal codes over cubic finite fields.

Contents

1 Preliminaries

Let us first fix some notation. We consider function fields F/K where K is the full constant field of F. In most cases, K will be a finite field $K = \mathbb{F}_\ell$ or its algebraic closure $K = \bar{\mathbb{F}}_\ell$. We denote by $\mathbb{P}(F)$ the set of places of F/K. For a place P of F/K, we will denote the normalized discrete valuation of F/K associated with P by v_P. For a rational function field $K(x)$ we will write $(x = a)$ for the place which is the zero of $x - a$ (where $a \in K$) and $(x = \infty)$ for the pole of x. For a place P of F/K of degree 1 and an element $x \in F$, we will denote by $x(P) \in K \cup \{\infty\}$ the value (=residue class) of the function x at the place P.

For a finite separable extension E of F and a place $Q \in \mathbb{P}(E)$ we will denote by $Q|_F$ the restriction of Q to F (i.e. $Q|_F = Q \cap F$). We will write $Q|P$, if the place $Q \in \mathbb{P}(E)$ lies over the place $P \in \mathbb{P}(F)$. In this case, we will denote by $e(Q|P)$ and $d(Q|P)$ the ramification index of $Q|P$ and the different exponent of $Q|P$, respectively.

A tower $\mathcal{F}$ of function fields over $\mathbb{F}_\ell$ is an infinite sequence $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ of function fields $F_i/\mathbb{F}_\ell$, having the following properties:

(i) $F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots$.

(ii) The field $\mathbb{F}_\ell$ is the full constant field of F_i, for $i = 0, 1, 2, \ldots$.

(iii) For each $i \geq 1$, the extension F_i/F_{i-1} is finite and separable.

(iv) $g(F_i) \to \infty$ as $i \to \infty$.

For a tower $\mathcal{F}$ over $\mathbb{F}_\ell$, it can be shown, that the following limit exists (see [6]):

$$\lambda(\mathcal{F}) := \lim_{i \to \infty} \frac{N(F_i)}{g(F_i)}$$

This real number $\lambda(\mathcal{F})$ is called the *limit of the tower* $\mathcal{F}$. Clearly,

$$0 \leq \lambda(\mathcal{F}) \leq A(\ell) \leq \sqrt{\ell} - 1.$$

A tower $\mathcal{F}$ over $\mathbb{F}_\ell$ is said to be

asymptotically good, if $\lambda(\mathcal{F}) > 0$,

asymptotically bad, if $\lambda(\mathcal{F}) = 0$.

asymptotically optimal, if $\lambda(\mathcal{F}) = A(\ell)$.

It is sometimes useful, to consider the asymptotic behaviour of the genus and the asymptotic behaviour of the number of rational places separately. Hence we define:

- The *genus* $\gamma(\mathcal{F})$ *of* $\mathcal{F}$ *over* F_0

$$\gamma(\mathcal{F}) := \lim_{i\to\infty} \frac{g(F_i)}{[F_i : F_0]}.$$

- The *splitting rate* $\nu(\mathcal{F})$ *of* $\mathcal{F}$ *over* F_0

$$\nu(\mathcal{F}) := \lim_{i\to\infty} \frac{N(F_i)}{[F_i : F_0]}.$$

It can be shown (see [7]), that these limits exist ($\gamma(\mathcal{F})$ can be ∞) and

$$0 < \gamma(\mathcal{F}) \leq \infty, \quad 0 \leq \nu(\mathcal{F}) \leq N(F_0) < \infty.$$

The tower $\mathcal{F}$ is asymptotically good if and only if $\gamma(\mathcal{F}) < \infty$ and $\nu(\mathcal{F}) > 0$, and in this case, $\lambda(\mathcal{F}) = \nu(\mathcal{F})/\gamma(\mathcal{F})$.

Let $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ and $\mathcal{E} = (E_0, E_1, E_2, \ldots)$ be towers of function fields over $\mathbb{F}_\ell$. Then the tower $\mathcal{F}$ is called a *subtower* of $\mathcal{E}$, if for each F_m, there exists an E_n, such that $F_m \subseteq E_n$. If $\mathcal{F}$ is a subtower of $\mathcal{E}$, we write $\mathcal{F} \prec \mathcal{E}$. We have the following Proposition:

Proposition 1.1. *Let* $\mathcal{F}$ *and* $\mathcal{E}$ *be towers over* $\mathbb{F}_\ell$. *Suppose* $\mathcal{F} \prec \mathcal{E}$; *i.e.* $\mathcal{F}$ *is a subtower of* $\mathcal{E}$. *Then*

(i) $\lambda(\mathcal{F}) \geq \lambda(\mathcal{E})$.

(ii) *If* $\mathcal{E}$ *is asymptotically good (resp. optimal), then* $\mathcal{F}$ *is asymptotically good (resp. optimal).*

(ii) *If* $\mathcal{F}$ *is asymptotically bad, then* $\mathcal{E}$ *is asymptotically bad.*

Proof. See [6]. □

Let $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ be a tower of function fields. A place P of F_0 is said to be *ramified in the tower* $\mathcal{F}$, if the place P is ramified in the extension F_i/F_0 for some $i \geq 1$. The set

$$V(\mathcal{F}/F_0) := \{P \in \mathbb{P}(F_0) | P \text{ is ramified in } \mathcal{F}\}$$

is called the *ramification locus of* $\mathcal{F}$ *over* F_0. This set plays an important role while determining the genus of the tower $\mathcal{F}$.

A rational place P of F_0 is said to *split completely in the tower* $\mathcal{F}$, if the place P splits completely in all extensions F_i/F_0. The set

$$Z(\mathcal{F}/F_0) := \{P \in \mathbb{P}(F_0) | \deg P = 1 \text{ and } P \text{ splits completely in } \mathcal{F}\}$$

is called the *splitting locus of* $\mathcal{F}$ *over* F_0. It is clear that $\nu(\mathcal{F}) \geq |Z(\mathcal{F})|$, where $|Z(\mathcal{F})|$ denotes the cardinality of the set $Z(\mathcal{F})$.

2 The Bezerra–Garcia–Stichtenoth tower

Let q be a prime power and $\ell = q^3$. Consider the BGS tower $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ of function fields over the finite field $\mathbb{F}_\ell$, which is defined recursively by the equation

$$y^q - y^{q-1} = 1 - x + \frac{1}{x^{q-1}}; \tag{2.1}$$

i.e., $F_0 = \mathbb{F}_\ell(x_0)$ is the rational function field and $F_{i+1} = F_i(x_{i+1})$, where

$$x_{i+1}^q - x_{i+1}^{q-1} = 1 - x_i + \frac{1}{x_i^{q-1}} \quad \text{for } i \geq 0. \tag{2.2}$$

In [2], the defining equation of this recursive tower was originally given as

$$\frac{1-\tilde{y}}{\tilde{y}^q} = \frac{\tilde{x}^q + \tilde{x} - 1}{\tilde{x}}. \tag{2.3}$$

After performing the transformation $\tilde{x} = x^{-1}$, $\tilde{y} = y^{-1}$, it is clear that Equation (2.1) and Equation (2.3) define the same tower.

2.1 Some basic properties of the BGS tower

Let us compile and prove some basic facts about the BGS tower. When we will be concerned with the genus of the BGS tower, for simplicity, we consider the same tower over the algebraic closure $\bar{\mathbb{F}}_\ell$ of $\mathbb{F}_\ell$, since the degree and the ramification behaviour of the extensions under consideration will not change under this constant field extension. Define the set

$$R := \{\alpha \in \bar{\mathbb{F}}_\ell \mid \alpha^q - \alpha^{q-1} = 1\}.$$

Lemma 2.1. (i) *The ramification indices in the first step of the tower (i.e. in the extension $\bar{\mathbb{F}}_\ell(x_0, x_1)/\bar{\mathbb{F}}_\ell(x_0)$) are as in Figure* 2.1.

(ii) *The places $(x_0 = 0), (x_0 = \infty)$ and $(x_0 = \alpha)$, with $\alpha \in R$, are the only places of $\bar{\mathbb{F}}_\ell(x_0)$ that are ramified in the extension $\bar{\mathbb{F}}_\ell(x_0, x_1)/\bar{\mathbb{F}}_\ell(x_0)$.*

(iii) *In the extension $\bar{\mathbb{F}}_\ell(x_0, x_1)/\bar{\mathbb{F}}_\ell(x_1)$, ramification indices and different exponents are as in Figure* 2.2.

(iv) *The places $(x_1 = \infty)$ and $(x_1 = \alpha)$, with $\alpha \in R$ are the only places of $\bar{\mathbb{F}}_\ell(x_1)$ that are ramified in the extension $\bar{\mathbb{F}}_\ell(x_0, x_1)/\bar{\mathbb{F}}_\ell(x_1)$.*

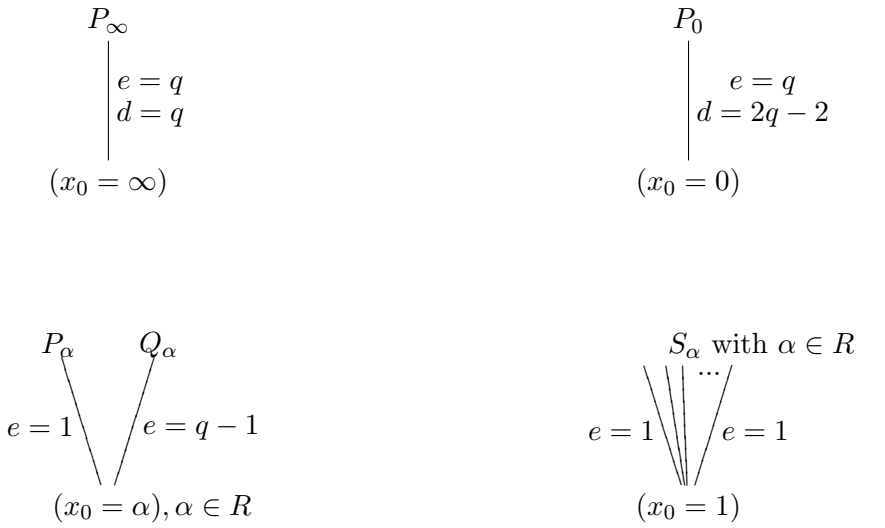

Figure 2.1:

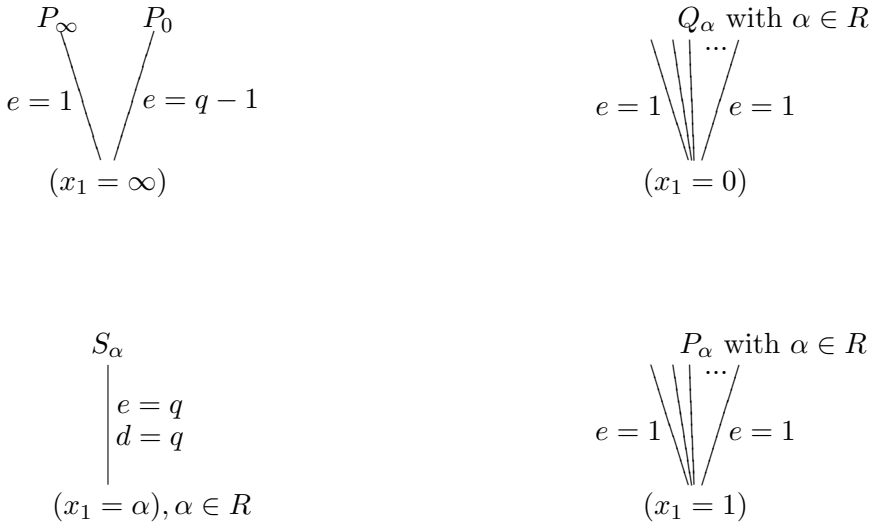

Figure 2.2:

(v) *In the function field* $\bar{\mathbb{F}}_\ell(x_0, x_1)$ *we have the following principal divisors:*

$$(x_0) = qP_0 - qP_\infty,$$

$$(x_0 - 1) = \sum_{\gamma \in R} S_\gamma - qP_\infty,$$

$$(x_0 - \alpha) = P_\alpha + (q-1)Q_\alpha - qP_\infty, \text{ for } \alpha \in R,$$

$$(x_1) = \sum_{\gamma \in R} Q_\gamma - P_\infty - (q-1)P_0,$$

$$(x_1 - 1) = \sum_{\gamma \in R} P_\gamma - P_\infty - (q-1)P_0,$$

$$(x_1 - \alpha) = qS_\alpha - P_\infty - (q-1)P_0, \text{ for } \alpha \in R.$$

(vi) *Let $r \geq 1$ and let Q be a place of F_r. For $0 \leq j \leq r-1$, the following holds for the values of the functions x_j, x_{j+1} at the place Q:*

- *if $x_j = \infty$, then $x_{j+1} = \infty$,*
- *if $x_j = 0$ then $x_{j+1} = \infty$,*
- *if $x_j = \alpha$ with $\alpha \in R$ then either $x_{j+1} = 0$ or $x_{j+1} = 1$,*
- *if $x_j = 1$ then $x_{j+1} = \alpha$ for some $\alpha \in R$.*

- *if $x_{j+1} = \infty$ then either $x_j = 0$ or $x_j = \infty$,*
- *if $x_{j+1} = 1$ then $x_j = \alpha$ for some $\alpha \in R$,*
- *if $x_{j+1} = 0$ then $x_j = \alpha$ for some $\alpha \in R$,*
- *if $x_{j+1} = \alpha$ with $\alpha \in R$ then $x_j = 1$.*

Proof. We only show the assertions concerning the different exponents of the wildly ramified places in items (i) and (iii). All other assertions follow easily from the defining Equation (2.2) of the tower.

Let P_∞ be a place of $\bar{\mathbb{F}}_\ell(x_0, x_1)$ lying over the place $(x_0 = \infty)$ of $\bar{\mathbb{F}}_\ell(x_0)$. Since, by Equation (2.2), $x_1^q - x_1^{q-1} = 1 - x_0 + 1/x_0^{q-1}$, it follows that $v_{P_\infty}(x_1) < 0$ and

$$q \cdot v_{P_\infty}(x_1) = v_{P_\infty}(x_1^q - x_1^{q-1}) = v_{P_\infty}(1 - x_0 + 1/x_0^{q-1}) = v_{P_\infty}(x_0) = -e(P_\infty \mid (x_0 = \infty)).$$

Since $e(P_\infty \mid (x_0 = \infty)) \leq [\bar{\mathbb{F}}_\ell(x_0, x_1) : \bar{\mathbb{F}}_\ell(x_0)] \leq q$, we obtain $e(P_\infty \mid (x_0 = \infty)) = q$ (hence $v_{P_\infty}(x_0) = -q$) and $v_{P_\infty}(x_1) = -1$. So the function $1/x_1$ is a prime element at P_∞. The minimal polynomial of $1/x_1$ over $\bar{\mathbb{F}}_\ell(x_0)$ is

$$\sigma(T) = T^q + \frac{1}{1 - x_0 + 1/x_0^{q-1}} \cdot T - \frac{1}{1 - x_0 + 1/x_0^{q-1}}$$

and therefore, by [20, Prop. III.5.12],

$$d(P_\infty \mid (x_0 = \infty)) = v_{P_\infty}(\sigma'(x_1^{-1})) = v_{P_\infty}(\frac{1}{1 - x_0 + 1/x_0^{q-1}}) = q.$$

In a similar way one shows that $d(P_0 \mid (x_0 = 0)) = 2q - 2$ and $d(S_\alpha \mid (x_1 = \alpha)) = q$ for $\alpha \in R$, using the fact that $x_0 \cdot x_1$ and $(x_0 - 1)$ are prime elements at the places P_0 and S_α, respectively. □

Lemma 2.2. *For all $i \geq 0$, we have*

(i) *The place $(x_0 = \infty)$ is totally ramified in the extension F_i/F_0, with ramification index $e = q^i$. The unique place of the function field F_i, which lies over the place $(x_0 = \infty)$ of F_0, is a simple pole of x_i.*

(ii) *The field $\mathbb{F}_\ell$ is algebraically closed in F_i, and $[F_i : F_0] = q^i$.*

Proof. (i) By induction: The case $i = 0$ is trivial. Assume that the assertion is true for some i. Let Q be a place of the function field F_{i+1} lying over the place $(x_0 = \infty)$ of F_0. Let P, P_1 and P_2 be the restrictions of Q to the subfields $\mathbb{F}_\ell(x_i)$, F_i and $\mathbb{F}_\ell(x_i, x_{i+1})$, respectively. By induction hypothesis, P is the pole of x_i in $\mathbb{F}_\ell(x_i)$ and $e(P_1 \mid P) = 1$. By Lemma 2.1, (i), (iii) and (vi), P_2 (and hence also Q) will be a pole of x_{i+1} with $e(P_2 \mid P) = q$ and $e(P_2 \mid (x_{i+1} = \infty)) = 1$. The assertion now follows from Abhyankar's Lemma (see [20, Ch. III.8]).
(ii) Clear by (i). □

Remark 2.3. For $q > 2$, the steps in the BGS tower are not Galois, as follows from the ramification behaviour of the place $(x_0 = \alpha)$ for $\alpha \in R$ in the extension $\bar{\mathbb{F}}_\ell(x_0, x_1)/\bar{\mathbb{F}}_\ell(x_0)$.

Lemma 2.4. *The ramification locus of $\mathcal{F}$ over F_0 (i.e., the set of places of the function field F_0, which are ramified in some extension F_n/F_0) is finite and is given by*

$$V(\mathcal{F}/F_0) = \{(x_0 = 0), (x_0 = \infty), (x_0 = 1)\} \cup \{(x_0 = \alpha) \mid \alpha \in R\}.$$

Proof. Let $P \in V(\mathcal{F}/F_0)$. Then, for some $n \geq 1$, there exists a place $Q \in \mathbb{P}(F_n)$ lying over P, such that Q is ramified in the extension F_n/F_{n-1}. By Abhyankar's Lemma, the restriction of Q to the subfield $\mathbb{F}_\ell(x_{n-1}, x_n)$ will be ramified in the extension $\mathbb{F}_\ell(x_{n-1}, x_n)/\mathbb{F}_\ell(x_{n-1})$. Therefore, by Lemma 2.1, (ii), we have $x_{n-1}(Q) = 0, \infty$ or α, with $\alpha \in R$. The assertion now follows from Lemma 2.1, (vi). □

2.2 The corresponding pyramid and the main difficulties

As above, we consider the BGS tower $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ over the algebraic closure $\bar{\mathbb{F}}_\ell$ of $\mathbb{F}_\ell$. Let $r \geq 1$. In order to estimate the genus of the function field F_r, it is necessary to investigate the ramification behaviour in the extension F_r/F_0 more thoroughly. Let Q be a place of F_r, which is ramified in the extension F_r/F_0. Let P be its restriction to F_0. We want to determine the ramification index $e(Q|P)$ and the different exponent $d(Q|P)$. We classify the ramified places of F_r/F_0 as follows: Consider the sequence $S(Q) = (x_0(Q), x_1(Q), \ldots, x_r(Q))$, where $x_i(Q) \in \bar{\mathbb{F}}_\ell \cup \{\infty\}$ denotes the value (=residue class) of the function x_i at the place Q. By Lemma 2.4 and Lemma 2.1 (vi) , the sequence $S(Q)$ belongs to one of the following types:

- Type I) $S(Q) = (\infty, \infty, \ldots, \infty)$.
- Type II) $S(Q) = (0, \infty, \infty, \ldots, \infty)$.
- Type III) $S(Q) = (\ldots, \alpha_k, 1, \alpha_{k+1}, \ldots, 1, \alpha_m, 0, \infty, \infty, \ldots, \infty)$ with $\alpha_i \in R$ (i.e., the first entries of $S(Q)$ alternate between 1 and elements of the set R, followed by $0, \infty, \infty, \ldots, \infty$).

For Type I, it is seen from Figure 2.1, Figure 2.2 and Abhyankar's Lemma that $e(Q|P) = q^r$ and $d(Q|P) = (q^{r+1} - q)/(q - 1)$. Similarly, for Type II, $e(Q|P) = q^r$ and $d(Q|P) = 2(q^r - 1)$.

Now we investigate places of Type III. In fact, this is the hard part of the paper [2]. For $0 \leq i \leq j \leq r$, let $F^{i,j} = \overline{\mathbb{F}}_\ell(x_i, x_{i+1}, \ldots, x_j)$. In particular, $F^{0,r} = F_r$. For $0 \leq i_1 \leq j_1 \leq r$ and $0 \leq i_2 \leq j_2 \leq r$, we have

$$F^{i_1,j_1} \text{ is a subfield of } F^{i_2,j_2} \Leftrightarrow i_2 \leq i_1 \text{ and } j_1 \leq j_2.$$

The arrangement of the subfields $F^{i,j}$ $(0 \leq i \leq j \leq r)$ of F_r is depicted in Figure 2.3.

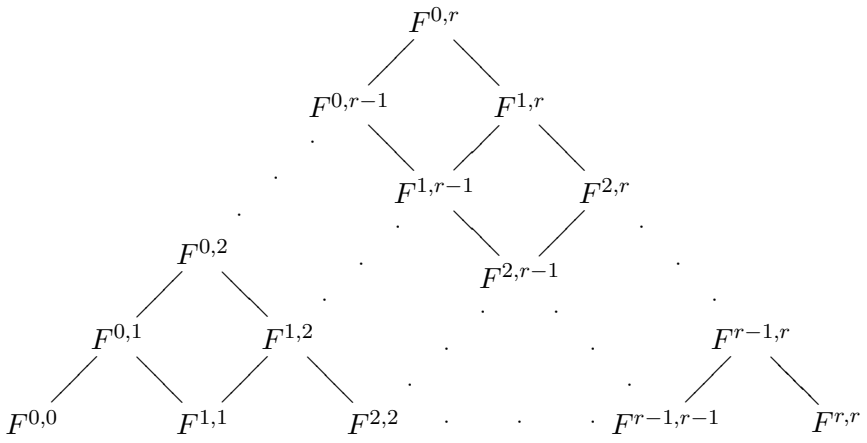

Figure 2.3: Arrangement of subfields $F^{i,j}$

Let Q be a place of F_r, which is ramified in the extension F_r/F_0 and which is of Type III. Denote by $Q^{i,j}$ the restriction of the place Q to $F^{i,j}$. Our aim is to estimate the ramification index $e(Q|Q^{0,0})$ and the different exponent $d(Q|Q^{0,0})$. We assume that $x_0(Q) = 1$ (the case $x_0(Q) \in R$ is analogous). Then there is some t with $1 \leq t \leq r$ such that

- $x_t(Q) = 0$,
- $x_1(Q) = \alpha_1, x_3(Q) = \alpha_3, \ldots, x_{t-1}(Q) = \alpha_{t-1}$, with $\alpha_1, \alpha_3, \ldots, \alpha_{t-1} \in R$,
- $x_0(Q) = x_2(Q) = \ldots = x_{t-2}(Q) = 1$,
- $x_i(Q) = \infty$ for $i > t$.

In order to study the ramification index and different exponent of Q over $(x_0 = 1)$, we investigate the behaviour of Q in all steps of the "pyramid" in Figure 2.3. However, ultimately we are only interested in the ramification behaviour along the left side of the pyramid; i.e., along the line EC in Figure 2.4.

From Lemma 2.1 (i) we immediately read off $e(Q^{i,i+1}|Q^{i,i})$ and $d(Q^{i,i+1}|Q^{i,i})$ for $0 \leq i \leq r-1$, since the extension $F^{i,i+1}/F^{i,i}$ corresponds just to the first step of the tower. Similarly, from Lemma 2.1 (iii), we obtain $e(Q^{i-1,i}|Q^{i,i})$ and $d(Q^{i-1,i}|Q^{i,i})$ for $1 \leq i \leq r$. This situation is depicted in Figure 2.5. For extensions, where the restriction of the place Q is wildly ramified, the different exponents are provided within square brackets.

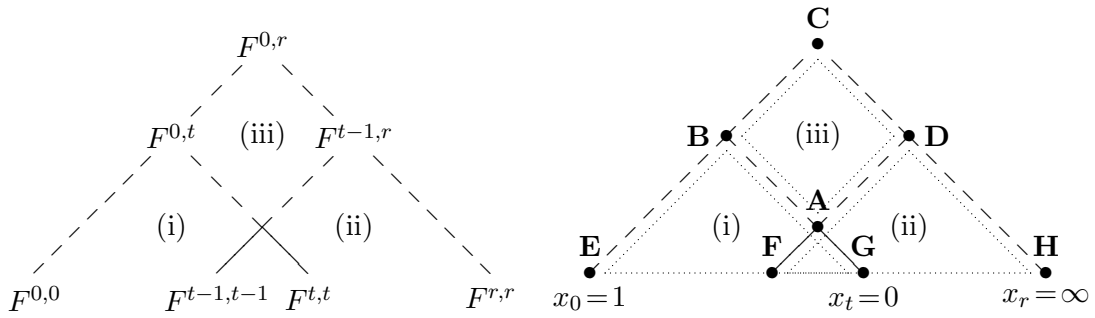

Figure 2.4:

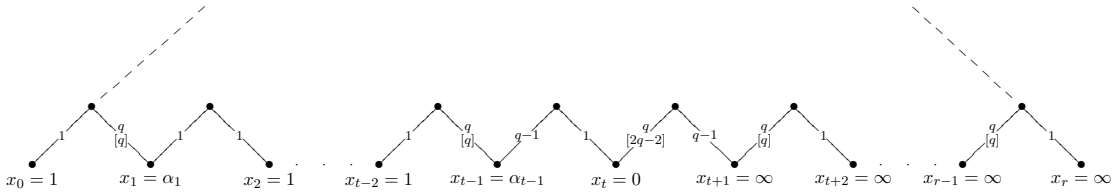

Figure 2.5:

As shown in Figure 2.4, we divide the pyramid corresponding to the field $F^{0,r}$ into three parts:

(i) the triangle EGB, which is the pyramid corresponding to the field $F^{0,t}$,

(ii) the triangle FHD, which is the pyramid corresponding to the field $F^{t-1,r}$,

(iii) the rectangle $ADCB$.

From Figure 2.5 and Abhyankar's Lemma one obtains easily the ramification indices and different exponents of Q in part (i), i.e. in the pyramid corresponding to the field $F_t = \bar{\mathbb{F}}_\ell(x_0, x_1, \ldots, x_t)$, as shown in Figure 2.6.

Likewise, the ramification behaviour of Q in part (ii), i.e. in the pyramid corresponding to the field $F^{t-1,r} = \bar{\mathbb{F}}_\ell(x_{t-1}, x_t, \ldots, x_r)$ follows from Figure 2.5 and Abhyankar's Lemma, and is depicted in Figure 2.7.

It remains to determine the ramification behaviour of the place Q in part (iii) of the pyramid of $F^{0,r}$, which is depicted in Figure 2.8. However, in composita, where the place is wildly ramified in both directions, Abhyankar's Lemma cannot be applied. These problematic composita are indicated in Figure 2.8 by dotted squares. Thus it is hard to determine the ramification behaviour along the line BC in Figure 2.8 and the major part of [2] is concerned with this situation. This is in fact also the main problem of this thesis.

Before studying these problematic composita in more detail, let us first investigate in the next section the rational places.

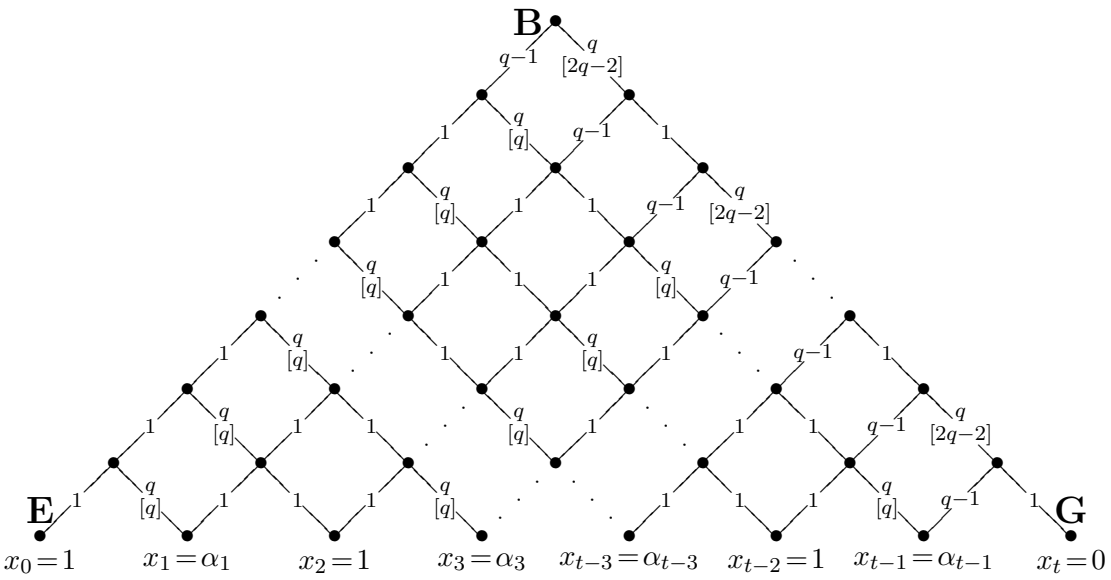

Figure 2.6:

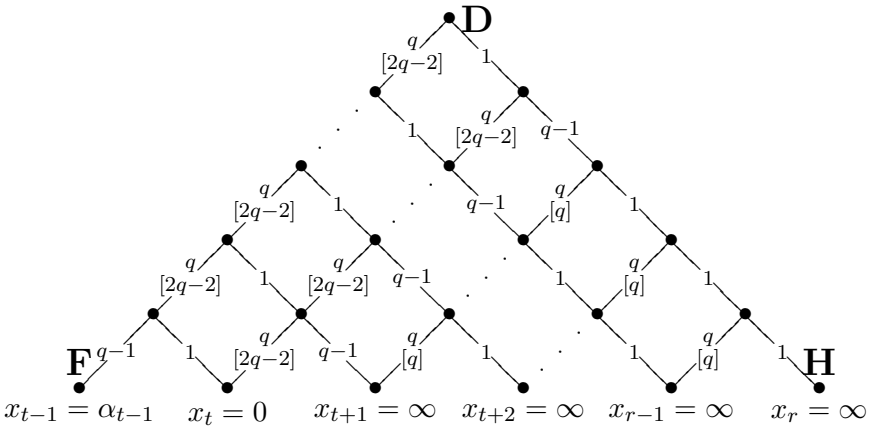

Figure 2.7:

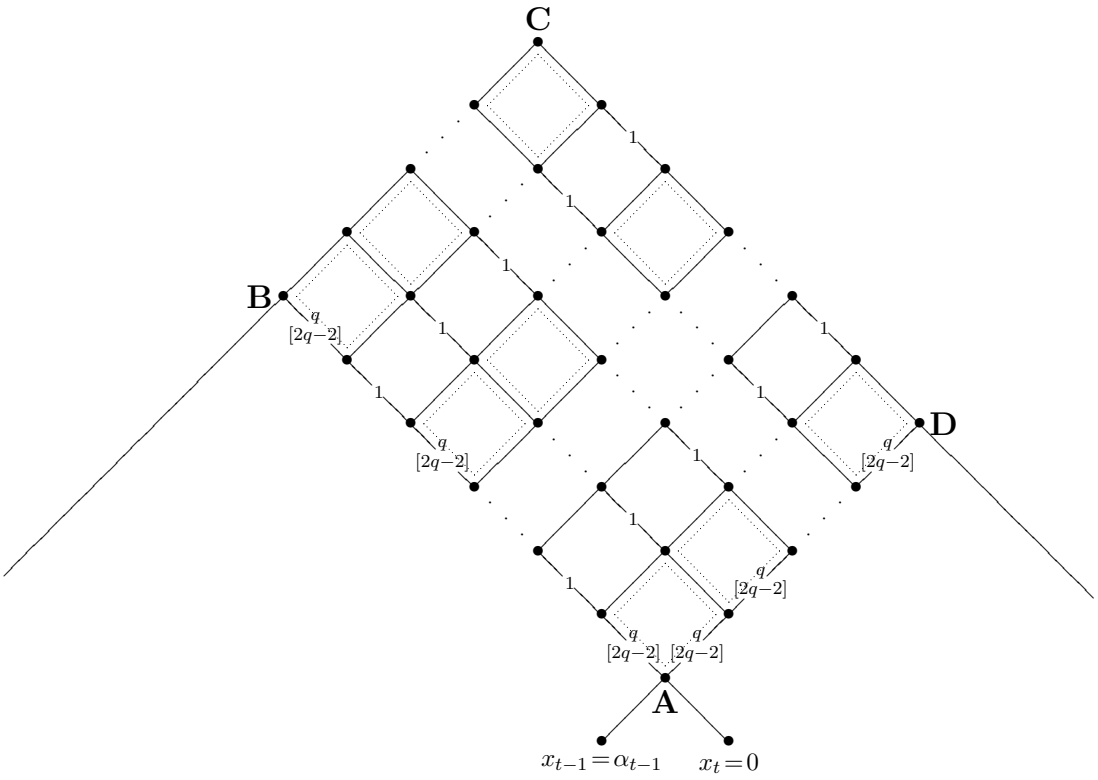

Figure 2.8:

2.3 Some rational places splitting completely in the tower

Next, we investigate some rational places of F_0, which split completely in all extensions F_i/F_0. Let

$$a(T) := T^q - T^{q-1} \quad \text{and} \quad b(T) := 1 - T + \frac{1}{T^{q-1}},$$

and let

$$\varphi(T) = T^{q+1} - T + 1.$$

We consider the following sets $S, A, B \in \bar{\mathbb{F}}_\ell$:

$$S := \{\gamma \in \bar{\mathbb{F}}_\ell \mid \varphi(\gamma) = 0\},$$

$$A := \{\gamma \in \bar{\mathbb{F}}_\ell \mid a(\gamma) \in S\} \quad \text{and} \quad B := \{\gamma \in \bar{\mathbb{F}}_\ell \mid b(\gamma) \in S\}.$$

Lemma 2.5. (i) $A = B$.

(ii) $|S| = q + 1$.

(iii) *For* $\gamma \in S$, $|a^{-1}(\gamma)| = q$ *and* $|A| = q \cdot (q + 1)$.

(iv) $A \subset \mathbb{F}_\ell$.

Proof. We have the following identity, which can be verified by direct calculation:

$$T \cdot \varphi(a(T)) = T^{q^2} \cdot \varphi(b(T)) = (T - 1)^{q^2+q+1} + 1 \tag{2.4}$$

(i) Follows directly from Equation (2.4), since for $\omega \in \bar{\mathbb{F}}_\ell \backslash \{0\}$, we have

$$\omega \in A \Leftrightarrow \varphi(a(\omega)) = 0 \Leftrightarrow \varphi(b(\omega)) = 0 \Leftrightarrow \omega \in B.$$

(ii) Clear, since the polynomial $\varphi(T)$ is separable.

(iii) Clear, since the polynomials $T^q - T^{q-1} - \gamma$ (for $\gamma \in S$) are separable and since $|S| = q + 1$ by (ii).

(iv) Let $\eta \in A$. Then $\varphi(a(\eta)) = 0$. So, by Equation (2.4), we have

$$(\eta - 1)^{q^2+q+1} + 1 = 0.$$

Therefore

$$(\eta - 1)^{q^2+q+1} = -1.$$

Since $\ell = q^3$, it follows that $\eta - 1 \in \mathbb{F}_\ell$ and hence $\eta \in \mathbb{F}_\ell$.

□

Theorem 2.6. *For $\omega \in A$, the place $(x_0 = \omega)$ of F_0 splits completely in the tower $\mathcal{F}/\mathbb{F}_\ell$. So there are at least $q(q+1)$ places of F_0, that split completely in the tower. Hence, the splitting rate*

$$\nu(\mathcal{F}) := \lim_{r\to\infty} \frac{N(F_r)}{[F_r : F_0]}$$

satisfies

$$\nu(\mathcal{F}) \geq q(q+1).$$

Proof. Let $\omega \in A$. By Lemma 2.5, the equation $a(\xi) = b(\omega)$ has exactly q roots ξ in $\bar{\mathbb{F}}_\ell$ and all of these roots are again in the set A and hence also in $\mathbb{F}_\ell$. The theorem follows now by induction. □

3 A simplified proof for the limit of the BGS tower

As mentioned above, the main difficulty in computing the limit of the BGS tower is to determine the ramification in composita, where the place is wildly ramified in both directions, since in this case Abhyankar's Lemma cannot be applied. A similar situation is considered in [4], where simpler proofs for the limits of the towers in [6, 8] are given. The main ingredient is a "key lemma" [4, Lemma 1], which also plays a crucial role in [5], where limits of the Galois closures of these towers are obtained. The main idea in [4] is contained in the following Proposition (see [5, Rem. 1.9 and Prop. 1.10]).

Proposition 3.1. *Let F/K be a function field, where K is a field of characteristic $p > 0$, let E_1 and E_2 finite Galois p-extensions of F and let $E = E_1 \cdot E_2$ be the composite field of E_1 and E_2. Let Q be a place of E. Let Q_1, Q_2 and P be the restrictions of Q to E_1, E_2 and F, respectively. If the different exponents $d(Q_i|P)$ satisfy*

$$d(Q_i|P) = 2(e(Q_i|P) - 1) \text{ for } i = 1, 2,$$

then $d(Q|Q_i) = 2(e(Q|Q_i) - 1)$ for $i = 1, 2$.

It would be desirable to use this Proposition also for the BGS tower, in order to simplify the computations. Unfortunately, since the extensions in this case are not Galois, Proposition 3.1 cannot be applied directly. However, Proposition 3.1 can be modified to obtain a simplified proof for the limit of the BGS tower. For this purpose, we make the following

Definition 3.2. Let K be an arbitrary field of characteristic $p > 0$, let F/K be a function field and let E be a finite separable extension of F. Let Q be a place of E and P be its restriction to F. We say that the place Q has property $(\star)$ for the extension E/F, if

$(\star_1)$ $d(Q|P) = 2(e(Q|P) - 1)$.

$(\star_2)$ There exists a finite separable extension H of F such that

- the place P is unramified in the extension H/F, and
- the extension HE/H is a Galois p-extension.

The definition is justified by the fact that in Proposition 3.1, instead of requiring the extension E_i/F to be a Galois p-extension, it is sufficient to make the weaker assumption that it has property $(\star)$ for the place Q_i. It turns out that this is indeed the case in all relevant cases in the BGS tower (see Lemma 3.9 below). So although the critical extensions in part (iii) (see Figure 2.8) are not Galois p-extensions, they have property $(\star)$ for the corresponding places.

We first prove the following generalization of Proposition 3.1:

Proposition 3.3. *Let F/K be a function field of characteristic $p > 0$, E_1 and E_2 finite separable extensions of F, $E = E_1 \cdot E_2$ the composite field of E_1 and E_2. Let Q be a place of E and Q_1, Q_2 and P be the restrictions of Q to E_1, E_2 and F, respectively. Suppose, that the places Q_i have property $(\star)$ for the extensions E_i/F $(i = 1, 2)$. Then the place Q has property $(\star)$ for the extension E/E_i for $i = 1, 2$.*

Proof. The place Q_i has property $(\star)$ for the extension E_i/F. So, let H_1 be an extension of F, s.t. the place P is unramified in H_1/F and H_1E_1/H_1 is a Galois p-extension. Let H_2 be the corresponding extension of F for Q_2 and E_2/F. Let $H = H_1 \cdot H_2$ be their compositum. Since the place P is unramified in H_1/F and H_2/F, it is unramified in the extension H/F. Moreover, since the lifting of a Galois extension with Galois group G is again Galois and its Galois group is a subgroup of G, HE_i/H will be a Galois p-extension for $i = 1, 2$. So, the extension H of F satisfies the conditions in Definition 3.2 for both Q_1 and Q_2 simultaneously.

Now lift everything by taking the compositum with H (see Figure 3.1). Since the place

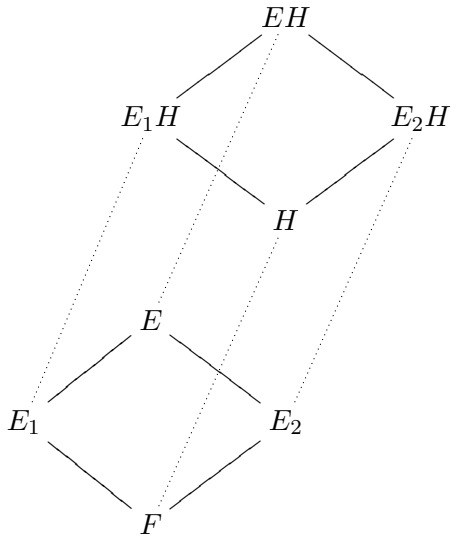

Figure 3.1: Lifting by H

P is unramified in the extension H/F, by Abhyankar's Lemma the places Q_1, Q_2 and Q will be unramified in the extensions E_1H/E_1, E_2H/E_2 and EH/E respectively. Hence, going up with H will not change the ramification behaviour. Since E_iH/H is a Galois p-extension for $i = 1, 2$, Proposition 3.1 can now be applied, so $d(Q|Q_i) = 2(e(Q|Q_i) - 1)$ for $i = 1, 2$. Moreover Q_i is unramified in the extension E_iH/E_i and EH/E_iH is a Galois p-extension for $i = 1, 2$. So the place Q has property $(\star)$ for the extensions E/E_1 and E/E_2. □

Remark 3.4. Let F/K be an algebraic function field of characteristic $p > 0$ and let E be a finite separable extension of F. Let Q be a place of E and let P be its restriction to F. Suppose that the place Q has property $(\star)$ for the extension E/F. Denote by $\widehat{E}_Q$ and $\widehat{F}_P$

the completions of the fields E and F at the places Q and P, respectively. Then it is easy to see that the extension $\widehat{E}_Q/\widehat{F}_P$ is a Galois p-extension and $d(\widehat{Q}|\widehat{P}) = 2(e(\widehat{Q}|\widehat{P})-1)$. So an alternative approach would be to consider the completion of the fields in the tower at relevant places and then to use a generalization of Lemma 3.1 to local fields, to determine the ramification behaviour in the tower. A proof of Lemma 3.1 for more general fields is given in Section 5.

We have to show, that all critical subextensions in Figure 2.8 have property ($\star$). By rewriting Equation (2.2), we immediately get the following

Lemma 3.5. (i) *$F^{i,j+1} = F^{i,j}(x_{j+1}) = F^{i,j}(1/x_{j+1})$ for $0 \le i \le j$, and the minimal polynomial of $1/x_{j+1}$ over $F^{i,j}$ is given by*

$$T^q + \frac{1}{1 - x_j + 1/x_j^{q-1}} \cdot T - \frac{1}{1 - x_j + 1/x_j^{q-1}} \in F^{i,j}[T].$$

(ii) *$F^{i-1,j} = F^{i,j}(x_{i-1}) = F^{i,j}(1/x_{i-1})$ for $1 \le i \le j$, and the minimal polynomial of $1/x_{i-1}$ over $F^{i,j}$ is given by*

$$T^q - (x_i^q - x_i^{q-1} - 1) \cdot T - 1 \in F^{i,j}[T].$$

Hence, by Lemma 3.5, each step of the pyramid in Figure 2.3 can be given in the form $F(y)/F$, where the irreducible polynomial of y over F is of the form $T^q + a \cdot T + b$, with $a, b \in F$. We have the following

Lemma 3.6. *Let $F/\bar{\mathbb{F}}_p$ be a function field, and let E=F(y) be an extension of F obtained from F by adjoining a root of the polynomial $T^{p^n} + a \cdot T + b$, with $a, b \in F^\times$. Let P be a place of F. If $(p^n - 1) \mid v_P(a)$, then condition ($\star_2$) of Definition 3.2 is satisfied; i.e., there exists an extension H of F, s.t. the place P is unramified in the extension H/F and EH/H is a Galois p-extension.*

Proof. Let H be the splitting field of the polynomial $T^{p^n} + a \cdot T$ over F (hence the extension H/F is Galois). Denote by Z the set of roots of $T^{p^n} + a \cdot T$. All roots of the polynomial $T^{p^n} + a \cdot T + b$ are of the form $y + \alpha$ with $\alpha \in Z \subset H$. It follows, that the lifting of E/F by H is a Galois extension. In fact, also the extension EH/F is Galois, since it is the splitting field of $T^{p^n} + a \cdot T$ and $T^{p^n} + a \cdot T + b$ over F.

Let σ be an automorphism of EH/H. Then $\sigma(y) = y + \alpha$, for some $\alpha \in Z$ and $\sigma^p(y) = y + p \cdot \alpha = y$. So $\sigma^p = id$, hence EH/H is a p-extension.

F contains a primitive $(p^n - 1)$-th root of unity. H/F is a Kummer extension of degree d, where $d \mid (p^n - 1)$ and H is obtained from F by adjoining a nonzero root of the polynomial $T^{p^n} + a \cdot T$. By the theory of Kummer extensions (see [20, Ch. III.7]), the condition $(p^n - 1) \mid v_P(a)$ implies that the place P is unramified in the extension H/F . □

Remark 3.7. In fact, EH is the Galois closure of the extension E/F.

Remark 3.8. The construction in Lemma 3.6 is a special case of the following more general situation: Let $a(T) \in F[T]$ be an additive separable polynomial; i.e., $a(T)$ is of the form $a_n T^{p^n} + a_n T^{p^{n-1}} + \cdots + a_1 T^p + a_0 T$, with $a_i \in F$, $a_0 \neq 0$. Consider the extension $E = F(y)$ of F obtained from F by adjoining an element y, which is a root of the polynomial $a(T) - u$, where u is an element of F. Let H be the splitting field of $a(T)$ over F. Then the extension EH/FH will be a Galois p-extension. However, in general it is not easy to give sufficient conditions for a place to be unramified in the splitting field of an additive polynomial.

Returning to the tower, let Q be a place of F_r ($r \geq 1$) which is ramified in the extension F_r/F_0 and which is of Type III; i.e., $x_t(Q) = 0$ for some $1 \leq t \leq r$ (see Figure 2.8). Then the restrictions of the place Q to the extension steps on the boundaries AB and AD have property ($\star$) for the corresponding extensions. More precisely, we have

Lemma 3.9.

a) For $0 \leq i \leq t-1$, let $M^i = F^{i,t} = \bar{\mathbb{F}}_\ell(x_i, x_{i+1}, \ldots, x_t)$ and $P^i = Q|_{M^i}$. The fields M^i correspond to the fields along the line AB in Figure 2.8. Then, for $0 \leq i \leq t-2$, the place P^i has property ($\star$) for the extension M^i/M^{i+1}.

b) For $t \leq i \leq r$, let $N^i = F^{t-1,i} = \bar{\mathbb{F}}_\ell(x_{t-1}, x_t, \ldots, x_i)$ and $R^i = Q|_{N^i}$ The fields N^i correspond to the fields along the line AD in Figure 2.8. Then, for $t+1 \leq i \leq r$, the place R^i has property ($\star$) for the extension N^i/N^{i-1}.

Proof. From Figure 2.8 we see immediately that for all extensions M^j/M^{j+1} ($0 \leq j \leq t-2$) and N^k/N^{k-1} ($t+1 \leq k \leq r$) (i.e. extension steps along the lines AB and AD) the restriction of the place Q is either totally ramified with ramification index $e = q$ and different exponent $d = 2q-2$, or unramified ($e = 1, d = 0$). In either case $d = 2(e-1)$. So it remains to show that ($\star_2$) holds.

a) Note that $M^i = M^{i+1}(x_i) = M^{i+1}(1/x_i)$. By Lemma 3.5 (ii), $1/x_i$ is a root of the polynomial

$$T^q - (x_{i+1}^q - x_{i+1}^{q-1} - 1) \cdot T - 1 \in M^{i+1}[T].$$

By Lemma 3.6, it suffices to show that

$$(q-1) \;\Big|\; v_{P^{i+1}}\Big(x_{i+1}^q - x_{i+1}^{q-1} - 1\Big).$$

Let $S^j = Q|_{\bar{\mathbb{F}}_\ell(x_j)}$, for $0 \leq j \leq t-1$. Note that $e(P^{i+1}|S^{i+1}) = q-1$ (see Figure 2.6). Since we have $x_{i+1}^q - x_{i+1}^{q-1} - 1 \in \bar{\mathbb{F}}_\ell(x_{i+1})$, it follows that

$$\begin{aligned} v_{P^{i+1}}\Big(x_{i+1}^q - x_{i+1}^{q-1} - 1\Big) &= e(P^{i+1}|S^{i+1}) \cdot v_{S^{i+1}}\Big(x_{i+1}^q - x_{i+1}^{q-1} - 1\Big) \\ &= (q-1) \cdot v_{S^{i+1}}\Big(x_{i+1}^q - x_{i+1}^{q-1} - 1\Big), \end{aligned}$$

so

$$(q-1) \;\Big|\; v_{P^{i+1}}\Big(x_{i+1}^q - x_{i+1}^{q-1} - 1\Big).$$

b) Let $W^j = Q|_{\bar{\mathbb{F}}_\ell(x_j)}$, for $t \le j \le r$. We have $N^i = N^{i-1}(x_i) = N^{i-1}(1/x_i)$. By Lemma 3.5 (i), $1/x_i$ is a root of the polynomial

$$T^q + \frac{1}{1 - x_{i-1} + 1/x_{i-1}^{q-1}} \cdot T - \frac{1}{1 - x_{i-1} + 1/x_{i-1}^{q-1}} \in N^{i-1}[T].$$

By Lemma 3.6, we have to show that

$$(q-1) \;\Big|\; v_{R^{i-1}}\Big(\frac{1}{1 - x_{i-1} + 1/x_{i-1}^{q-1}}\Big).$$

If $i > t+1$, this is clear, since in this case $\frac{1}{1-x_{i-1}+1/x_{i-1}^{q-1}} \in \bar{\mathbb{F}}_\ell(x_{i-1})$ and $e(R^{i-1}|W^{i-1}) = q-1$ (see Figure 2.7). So

$$v_{R^{i-1}}\Big(\frac{1}{1 - x_{i-1} + 1/x_{i-1}^{q-1}}\Big) = (q-1) \cdot v_{W^{i-1}}\Big(\frac{1}{1 - x_{i-1} + 1/x_{i-1}^{q-1}}\Big).$$

If $i = t+1$, then $e(R^{i-1}|W^{i-1}) = 1$. However in this case $W^{i-1} = Q|_{\bar{\mathbb{F}}_\ell(x_{i-1})} = (x_{i-1} = 0)$ is the zero of x_{i-1} in $\bar{\mathbb{F}}_\ell(x_{i-1})$. So

$$\begin{aligned} &v_{R^{i-1}}\Big(\frac{1}{1 - x_{i-1} + 1/x_{i-1}^{q-1}}\Big) \\ &= e(R^{i-1}|(x_{i-1} = 0)) \cdot v_{(x_{i-1}=0)}\Big(\frac{1}{1 - x_{i-1} + 1/x_{i-1}^{q-1}}\Big) = 1 \cdot (q-1), \end{aligned}$$

which is divisible by $q-1$. □

Theorem 3.10. *With notation as above, we have*

$$d(Q \mid Q|_{\bar{\mathbb{F}}_\ell(x_0,\ldots,x_t)}) = 2(e(Q \mid Q|_{\bar{\mathbb{F}}_\ell(x_0,\ldots,x_t)}) - 1).$$

Proof. Follows directly by Lemma 3.9, iterated application of Proposition 3.3 and transitivity of different exponents and ramification indices in towers. □

Theorem 3.11.

$$\gamma(\mathcal{F}) = \lim_{r\to\infty} \frac{g(F_r)}{[F_r : F_0]} \le \frac{q(q+2)}{2(q-1)}.$$

Proof. The degree of the different of F_r/F_0 is given by

$$\deg \mathrm{Diff}\ (F_r/F_0) = \sum_{P\in\mathbb{P}(F_0)} \sum_{\substack{P'\in\mathbb{P}(F_r)\\ P'|P}} d(P'|P) = \sum_{P\in V(\mathcal{F}/F_0)} \sum_{\substack{P'\in\mathbb{P}(F_r)\\ P'|P}} d(P'|P).$$

• The place $(x_0 = \infty)$ of F_0 is totally ramified in every extension in the tower. Let U_∞ be the unique place of F_r lying over it. U_∞ is of Type I (see Section 2), so

$$e(U_\infty|(x_0 = \infty)) = q^r \quad \text{and} \quad d(U_\infty|(x_0 = \infty)) = \frac{q^{r+1} - q}{q-1}.$$

• The place $(x_0 = 0)$ of F_0 is totally ramified in every extension of the tower. Let U_0 be the unique place of F_r lying over it. U_0 is of Type II, so

$$e(U_0|(x_0 = 0)) = q^r \quad \text{and} \quad d(U_0|(x_0 = 0)) = 2(q^r - 1).$$

• To estimate the contribution to $\deg \mathrm{Diff}\ (F_r/F_0)$ of places of F_r lying over places of F_0 in the set $\Phi := V(\mathcal{F}/F_0)\backslash\{(x_0 = 0), (x_0 = \infty)\}$, let

$$\Gamma_s = \{P \in \mathbb{P}(F_s) \mid P|_{\bar{\mathbb{F}}_\ell(x_s)} = (x_s = 0)\}.$$

Since for any $P \in \Gamma_s$, the ramification index is given by $e(P|(x_s = 0)) = q^{\lfloor s/2 \rfloor}$ (where $\lfloor t \rfloor$ denotes the greatest integer not exceeding t), we have

$$[F_s : \bar{\mathbb{F}}_\ell(x_s)] = q^s = q^{\lfloor s/2 \rfloor} \cdot |\Gamma_s|, \quad \text{so} \quad |\Gamma_s| = \frac{q^s}{q^{\lfloor s/2 \rfloor}}.$$

It follows that

$$\begin{aligned}
&\sum_{P \in \Phi} \sum_{\substack{P' \in \mathbb{P}(F_r) \\ P'|P}} d(P'|P) = \sum_{s=1}^{r} \sum_{\widetilde{P} \in \Gamma_s} \sum_{\substack{P' \in \mathbb{P}(F_r) \\ P'|\widetilde{P}}} d(P' \mid P'|_{F_0}) \\
&= \sum_{s=1}^{r} \sum_{\widetilde{P} \in \Gamma_s} \sum_{\substack{P' \in \mathbb{P}(F_r) \\ P'|\widetilde{P}}} \Big(d(\widetilde{P} \mid \widetilde{P}|_{F_0}) \cdot e(P'|\widetilde{P}) + d(P'|\widetilde{P}) \Big) \\
&= \sum_{s=1}^{r} \sum_{\widetilde{P} \in \Gamma_s} \sum_{\substack{P' \in \mathbb{P}(F_r) \\ P'|\widetilde{P}}} \Big((q-2) \cdot e(P'|\widetilde{P}) + 2(e(P'|\widetilde{P}) - 1) \Big) \\
&\le \sum_{s=1}^{r} \sum_{\widetilde{P} \in \Gamma_s} q \cdot \sum_{\substack{P' \in \mathbb{P}(F_r) \\ P'|\widetilde{P}}} e(P'|\widetilde{P}) = \sum_{s=1}^{r} \sum_{\widetilde{P} \in \Gamma_s} q \cdot [F_r : F_s] \\
&= \sum_{s=1}^{r} |\Gamma_s| \cdot q \cdot q^{r-s} = q^{r+1} \cdot \sum_{s=1}^{r} \frac{1}{q^{\lfloor s/2 \rfloor}} \le q^{r+1} \cdot \sum_{s=1}^{\infty} \frac{1}{q^{\lfloor s/2 \rfloor}} = \frac{q^{r+2} + q^{r+1}}{q-1}.
\end{aligned}$$

So, the degree of the different satisfies

$$\begin{aligned}
\deg \mathrm{Diff}(F_r/F_0) &\le \frac{q^{r+1} - q}{q-1} + 2(q^r - 1) + \frac{q^{r+2} + q^{r+1}}{q-1} \\
&= \frac{q^{r+2} + 4q^{r+1} - 2q^r - 3q + 2}{q-1} \le \frac{q^{r+2} + 4q^{r+1} - 2q^r}{q-1}.
\end{aligned}$$

Using Hurwitz genus formula, we get

$$2g(F_r) - 2 = -2q^r + \deg \mathrm{Diff}(F_r/F_0) \le \frac{q^{r+2} + 2q^{r+1}}{q-1}.$$

Therefore,

$$\lim_{r\to\infty} \frac{g(F_r)}{[F_r : F_0]} \leq \frac{q(q+2)}{2(q-1)}.$$

□

As an immediate consequence we obtain the main result of [2]:

Theorem 3.12. *The limit of the BGS tower $\mathcal{F}/\mathbb{F}_\ell$, where $\ell = q^3$, satisfies*

$$\lambda(\mathcal{F}) = \lim_{r\to\infty} \frac{N(F_r)}{g(F_r)} \geq \frac{2(q^2-1)}{q+2}.$$

Proof. Using Theorem 2.6 and Theorem 3.11, we obtain

$$\lambda(\mathcal{F}) = \frac{\nu(\mathcal{F})}{\gamma(\mathcal{F})} \geq \frac{2(q^2-1)}{q+2}.$$

□

4 The Galois closure of the BGS tower

Next, we want to investigate the Galois closure of the BGS tower. The Galois closure of a tower is defined as follows (see also [5]):

Let $\mathcal{F} = (F_n)_{n\geq 0}$ be a tower of function fields over $\mathbb{F}_\ell$. Let E_i be the Galois closure of the extension F_i/F_0, for $i = 0, 1, 2, \ldots$. Then the infinite sequence of function fields

$$\mathcal{E} = (E_0, E_1, \ldots)$$

is called the *Galois closure of $\mathcal{F}$ over F_0*.

Note that $E_0 = F_0$. We have the following Proposition (see [5, Prop. 2.1]):

Proposition 4.1. *Let $\mathcal{F}$ be a tower of function fields over $\mathbb{F}_\ell$, which has a nonempty splitting locus (i.e. $Z(\mathcal{F}) \neq \varnothing$). Then*

(i) *The Galois closure $\mathcal{E}$ of $\mathcal{F}$ is a tower over $\mathbb{F}_\ell$; i.e. the field $\mathbb{F}_\ell$ is algebraically closed in E_i for all $i = 0, 1, 2, \ldots$.*

(ii) $Z(\mathcal{E}/F_0)$=$Z(\mathcal{F}/F_0)$.

(iii) $V(\mathcal{E}/F_0) = V(\mathcal{F}/F_0)$.

Proof. See [5]. □

Let $\mathcal{F}$ be a tower over $\mathbb{F}_\ell$, and suppose that its Galois closure $\mathcal{E}$ is again a tower over $\mathbb{F}_\ell$. Then $\mathcal{F}$ will be a subtower of $\mathcal{E}$, and by Proposition 1.1, we have

$$\lambda(\mathcal{E}) \leq \lambda(\mathcal{F}).$$

Now, let $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ be the BGS tower over $\mathbb{F}_\ell$, as defined above by Equation 2.1. Let $\mathcal{E} = (E_0, E_1, E_2, \ldots)$ be the Galois closure of $\mathcal{F}$ over F_0. Note that $E_0 = F_0 = \mathbb{F}_\ell(x_0)$. Since the tower $\mathcal{F}$ has a nonempty splitting locus over F_0, by Proposition 4.1 it follows that $\mathcal{E}$ is also a tower over $\mathbb{F}_\ell$. Furthermore, $V(\mathcal{E}/F_0) = V(\mathcal{F}/F_0)$ and $Z(\mathcal{E}/F_0) = Z(\mathcal{F}/F_0)$.

We are interested in the limit of the Galois closure $\mathcal{E}$ of the BGS tower. In order to determine the limit of the tower, we again consider the splitting rate $\nu(\mathcal{E})$ and the genus $\gamma(\mathcal{E})$ of the tower separately. The first problem is easy:

Since $Z(\mathcal{E}/F_0) = Z(\mathcal{F}/F_0)$, from Theorem 2.6 we see that there are at least $q(q+1)$ places of E_0, that split completely in the tower $\mathcal{E}$. Hence, we have the following Proposition:

Proposition 4.2. *Let $\mathcal{E} = (E_0, E_1, E_2, \ldots)$ be the Galois closure of the BGS tower. Then the splitting rate $\nu(\mathcal{E})$ of $\mathcal{E}$ satisfies*

$$\nu(\mathcal{E}) = \lim_{i\to\infty} \frac{N(E_i)}{[E_i : E_0]} \geq |Z(\mathcal{E}/F_0)| \geq q(q+1).$$

Next, we want to investigate the genus $\gamma(\mathcal{E})$ of the tower $\mathcal{E}$. Again, to estimate the genus of the function field E_i with $i \geq 1$, we study the ramification behaviour in the extension E_i/E_0 in detail. Since we are interested in the ramification behaviour, we will consider for simplicity the same tower over the algebraic closure $K = \bar{\mathbb{F}}_\ell$ of $\mathbb{F}_\ell$.

Let $\Phi \supseteq E_0$ be a fixed algebraically closed field. Let $r \geq 1$. Then

$$E_r = \sigma_1(F_r)\sigma_2(F_r)\cdots\sigma_s(F_r),$$

where $\sigma_1, \sigma_2 \ldots, \sigma_s$ are the embeddings of F_r into Φ over F_0 (see Figure 4.1). Let Q

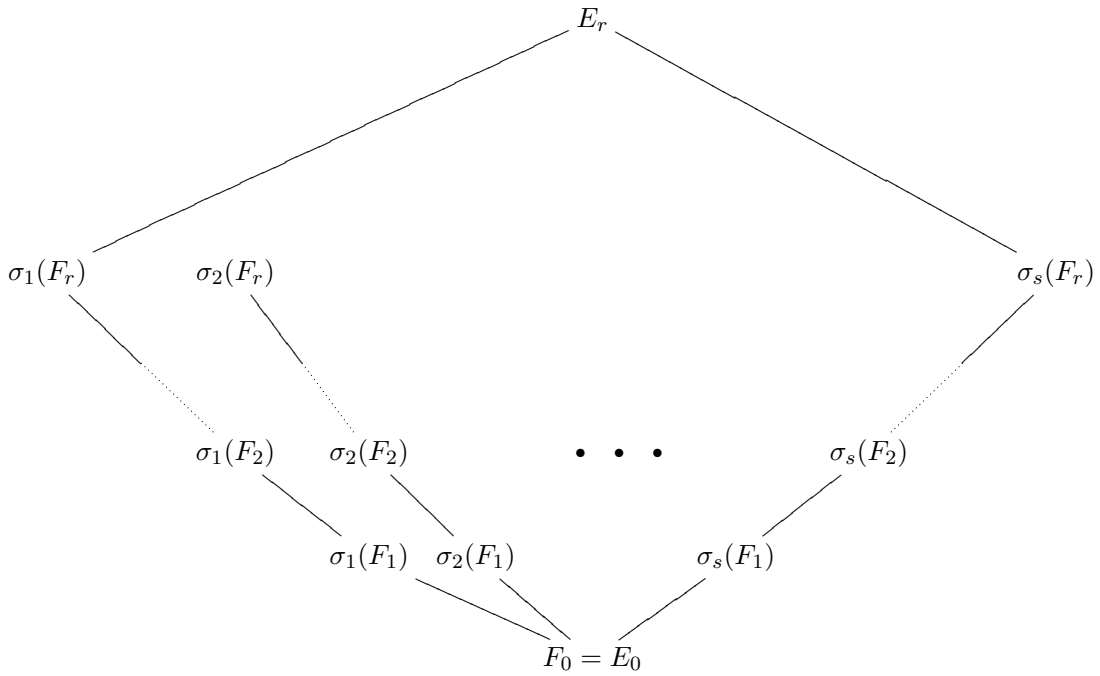

Figure 4.1: $E_r = \sigma_1(F_r)\sigma_2(F_r)\cdots\sigma_s(F_r)$,

be a place of E_r, which is ramified in the extension E_r/E_0. Let $P = Q|_{E_0}$. Above, we considered the ramification behaviour of the place P in the extensions $\sigma_j(F_r)/F_0$, $1 \leq j \leq s$ in detail. Now, our aim is to determine the ramification behaviour of the place P in the compositum E_r of $\sigma_1(F_r), \sigma_2(F_r), \ldots \sigma_s(F_r)$. Clearly, $P \in V(\mathcal{E}/E_0)$. By Lemma 2.4 and Proposition 4.1, the ramification locus of $\mathcal{E}$ is given by

$$V(\mathcal{E}/E_0) = V(\mathcal{F}/F_0) = \{(x_0 = 0), (x_0 = \infty), (x_0 = 1)\} \cup \{(x_0 = \alpha) \mid \alpha \in R\},$$

where $R = \{\alpha \in \bar{\mathbb{F}}_\ell \mid \alpha^q - \alpha^{q-1} = 1\}$. We will consider the three cases $P = (x_0 = 0), P = (x_0 = \infty)$ and $P \in \{(x_0 = 1)\} \cup \{(x_0 = \alpha) \mid \alpha \in R\}$ separately.

Proposition 4.3. *For $r \geq 1$, let Q be a place of E_r, such that $P = Q|_{E_0} = (x_0 = 0)$. Then $d(Q|P) = 2(e(Q|P) - 1)$.*

Proof. For $0 \leq i \leq r$, $1 \leq j \leq s$, let $Q_{j,i} = Q|_{\sigma_j(F_i)}$. In Section 2 we have seen that the place P is totally ramified in the extension $\sigma_j(F_r)/F_0$, it is a place of type II, $Q_{j,i+1}$ is a pole of $\sigma_j(x_{i+1})$, $e(Q_{j,i+1}|Q_{j,i}) = q$ and $d(Q_{j,i+1}|Q_{j,i}) = 2q-2$ for $0 \leq i \leq r-1$, $1 \leq j \leq s$. This situation is depicted in Figure 4.2.

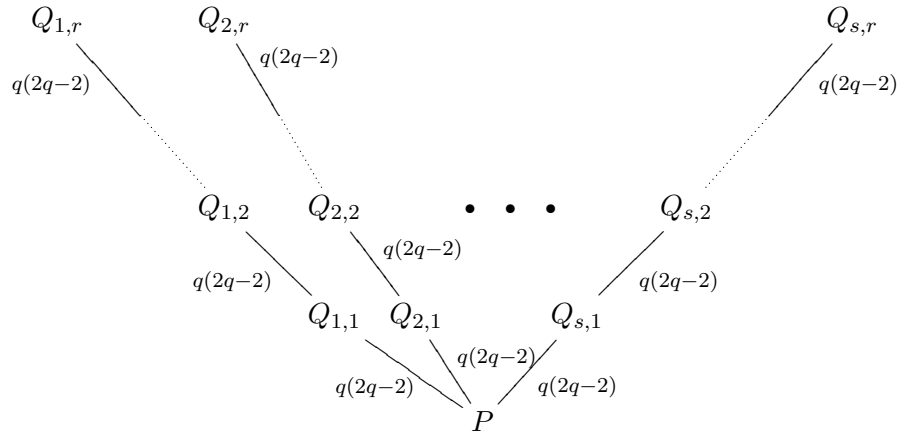

Figure 4.2: $P = (x_0 = 0)$

It was shown in Lemma 3.9, that the place $Q_{j,i+1}$ has property $(\star)$ for the extension $\sigma_j(F_{i+1})/\sigma_j(F_i)$, for $0 \leq i \leq r-1$, $1 \leq j \leq s$. By repeated application of Proposition 3.3 and transitivity of different exponents and ramification indices in towers, we see immediately, that $d(Q|P) = 2(e(Q|P)-1)$. □

Next we consider the the ramification behaviour of the place $P = (x_0 = \infty)$ in the extension E_r/E_0.

Proposition 4.4. *For $r \geq 1$, let Q be a place of E_r, such that $P = Q|_{E_0} = (x_0 = \infty)$. Then*

$$d(Q|P) \leq \frac{q}{q-1} e(Q|P).$$

Proof. Let $F_{-1} = F_0(x_{-1})$, where

$$1 - x_{-1} + \frac{1}{x_{-1}^{q-1}} = x_0^q - x_0^{q-1};$$

i.e. starting at $E_0 = F_0 = K(x_0)$, construct one step of the dual tower of $\mathcal{F}$. By Lemma 2.1 (iii), there exists a place R of $K(x_{-1}, x_0)/K(x_0)$ lying over the place $P = (x_0 = \infty)$ of $K(x_0)$, such that $e(R|P) = q-1$. Let S be a place of the composite field E_rF_{-1} lying over the place R and let Q' be the restriction of S to the subfield E_r (see Figure 4.3).

For $0 \leq i \leq r$, $1 \leq j \leq s$, let $Q'_{j,i} = Q'|_{\sigma_j(F_i)}$. As we have seen in Section 2, the place P is totally ramified in the extension $\sigma_j(F_r)/F_0$, it is a place of type I, $Q'_{j,i+1}$ is a zero of $\sigma_j(x_{i+1})$, $e(Q'_{j,i+1}|Q'_{j,i}) = q$ and $d(Q'_{j,i+1}|Q'_{j,i}) = q$ for $0 \leq i \leq r-1$, $1 \leq j \leq s$. This situation is depicted in Figure 4.4.

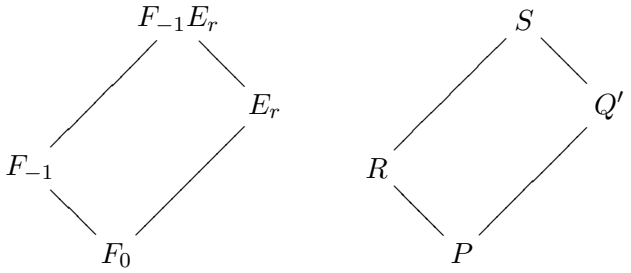

Figure 4.3:

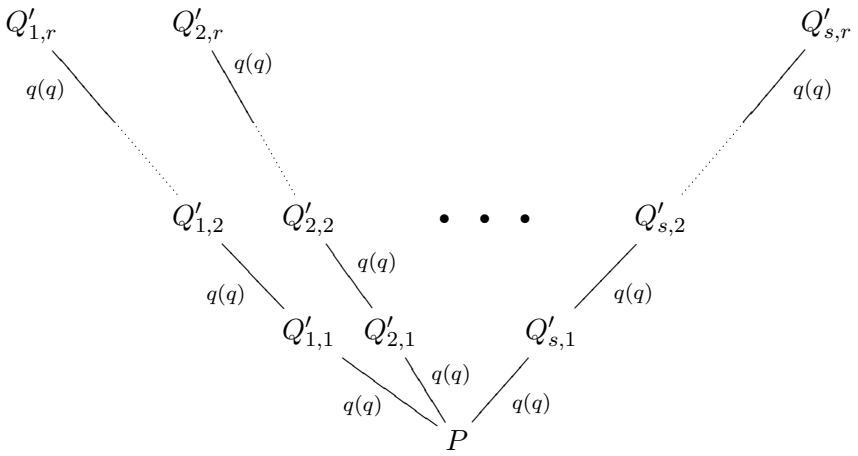

Figure 4.4: $P = (x_0 = \infty)$

Now lift everything by F_{-1} (see Figure 4.5). The restriction of the place S to $F_{-1}\sigma_j(F_{i+1})$ has property $(\star)$ for the extension $F_{-1}\sigma_j(F_{i+1})/F_{-1}\sigma_j(F_i)$ for $0 \leq i \leq r-1$, $1 \leq j \leq s$ (this follows by Abhyankar's Lemma and the same reasoning as in the proof of Lemma 3.9). By repeated application of Lemma 3.3 and transitivity of different exponents and ramification indices in towers, we obtain $d(S|R) = 2(e(S|R) - 1)$.

By using transitivity of different exponents and ramification indices in towers, we get

$$\begin{aligned} d(Q'|P) &= \frac{d(R|P)e(S|R) + d(S|R) - d(S|Q')}{e(S|Q')} \leq \frac{(q-2)e(S|R) + 2(e(S|R)-1)}{e(S|Q')} \\ &= \frac{q \cdot e(S|R) - 2}{e(S|Q')} \leq \frac{q \cdot e(S|R)}{e(S|Q')} = \frac{q \cdot e(S|R)}{(q-1)e(S|R)/e(Q'|P)} = \frac{q}{q-1}e(Q'|P) \end{aligned}$$

(see Figure 4.6).

Q and Q' are places of E_r lying over the place P of E_0 and since E_r/E_0 is a Galois extension, they will have the same ramification behaviour. Consequently,

$$d(Q|P) = d(Q'|P) \leq \frac{q}{q-1}e(Q'|P) = \frac{q}{q-1}e(Q|P).$$

□

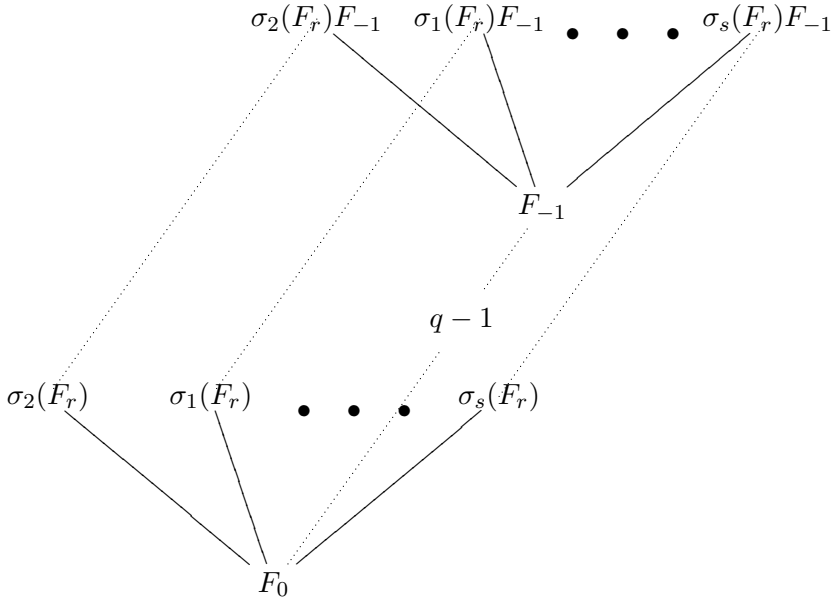

Figure 4.5:

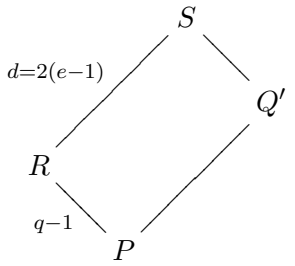

Figure 4.6:

Next, let Q be a place of E_r and let $P = Q|_{E_0}$ be its restriction to E_0. Assume that $P \in \{(x_0 = 1)\} \cup \{(x_0 = \alpha) \mid \alpha \in R\}$.

In Section 2, we studied the ramification of the place Q in the extension $\sigma_j(F_r)/F_0$. Suppose that the restriction of Q to $\sigma_j(F_r)$ is ramified over F_0. It is a place of type III. Furthermore, for some index t, with $1 \leq t \leq r$, we have:

- The restriction of Q to $\sigma_j(F_{t-1})$ is unramified over F_0.
- The restriction of Q to $\sigma_j(F_t)$ is tamely ramified over $\sigma_j(F_{t-1})$, with ramification index $q-1$.
- For $t < i \leq r$, the restriction of Q to $\sigma_j(F_i)$ has property $(\star)$ for the extension $\sigma_j(F_i)/\sigma_j(F_{i-1})$ (this follows from Lemma 3.9 and repeated application of Proposition 3.3).

To determine the ramification behaviour of the place Q in the extension E_r/E_0 we

have to consider the compositum of the $\sigma_j(F_r)$ with $1 \leq j \leq s$, where the restriction of the place Q has the properties above for each of these extensions $\sigma_j(F_r)/F_0$. So the following Lemma will be helpful:

Lemma 4.5. *Let F be a function field over $\bar{\mathbb{F}}_\ell$ and let F_1 and F_2 be finite separable extensions of F. Let $F' = F_1F_2$ be the compositum of F_1 and F_2. Let Q be a place of F', and let P_1, P_2 and P be its restrictions to F_1, F_2 and F, respectively. Suppose that the ramification behaviour of P_1 and P_2 over P are of the form above, i.e. they are first unramified, then tamely ramified with ramification index $q-1$ and then follows a sequence of extensions with the restriction of Q_i having property $(\star)$. Then the ramification behaviour of Q over P is also of the same form.*

Proof. This is clear by Abhyankar's Lemma and Proposition 3.3. See Figure 4.7 (consider the sequence of intermediate fields along the arrow in the Figure). Note that by abuse of language, we consider extensions, where the restriction of the place Q is unramified also as extensions where the restriction of Q has property $(\star)$. □

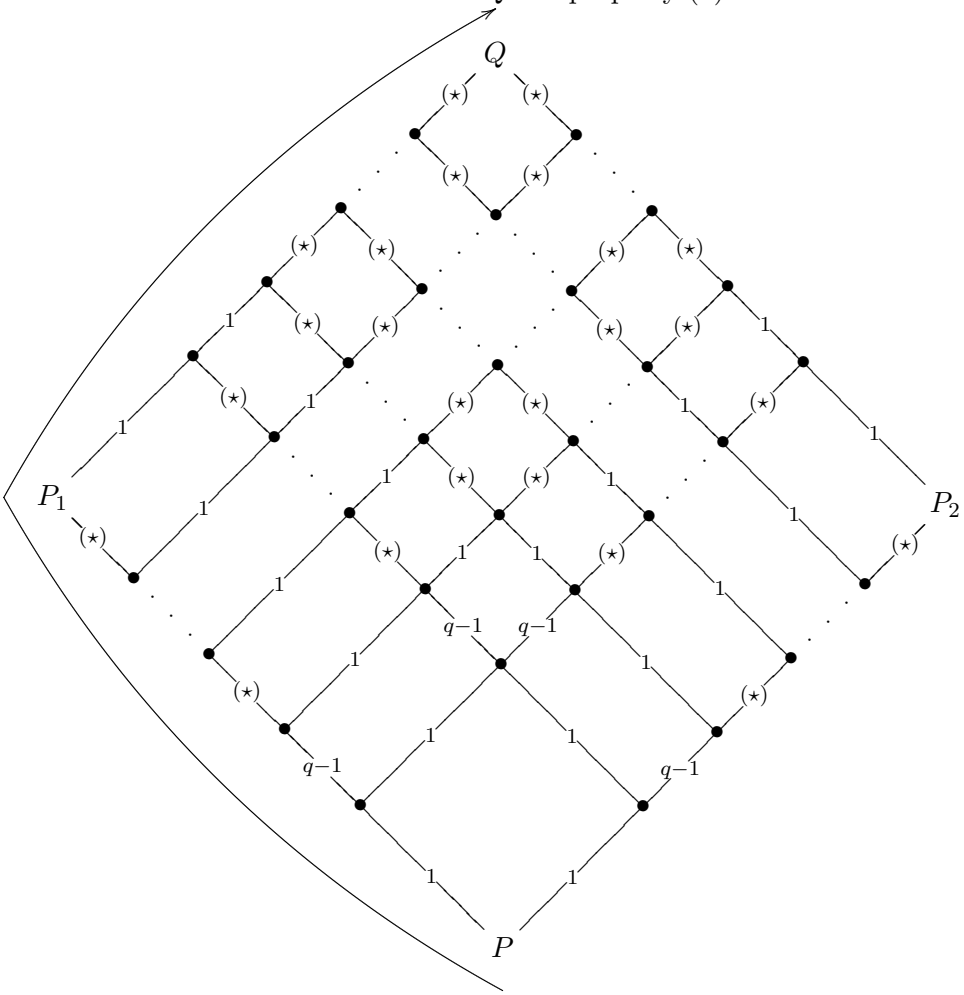

Figure 4.7:

Proposition 4.6. *Let Q be a place of E_r, such that $P = Q|_{E_0} \in \{(x_0 = 1)\} \cup \{(x_0 = \alpha) \mid \alpha \in R\}$. Then*

$$d(Q|P) \leq \frac{q}{q-1} e(Q|P).$$

Proof. By repeated application of Lemma 4.5 and by transitivity of different exponents and ramification indices in towers, we see that there are intermediate fields $E_0 \subseteq K \subset L \subseteq E_r$, such that $d(Q \mid Q|_L) = 2e(Q \mid Q|_L) - 2$, $e(Q|_L \mid Q|_K) = q-1$ and $e(Q|_K \mid P) = 1$, see Figure 4.8.

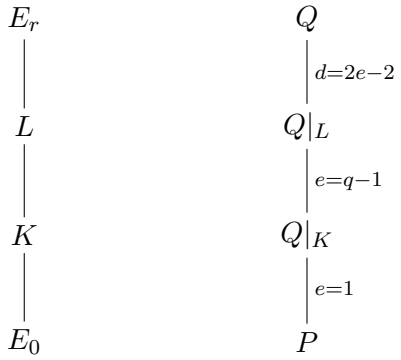

Figure 4.8:

Then

$$\begin{aligned} d(Q|P) &= d(Q|_L \mid Q|_K) e(Q \mid Q|_L) + d(Q \mid Q|_L) = (q-2) e(Q \mid Q|_L) + 2e(Q \mid Q|_L) - 2 \\ &= q \cdot e(Q \mid Q|_L) - 2 \leq \frac{q}{q-1}(q-1) e(Q \mid Q|_L) = \frac{q}{q-1} e(Q|P). \end{aligned}$$

□

Theorem 4.7. *Let $\mathcal{E} = (E_0, E_1, E_2, \ldots)$ be the Galois closure of the BGS tower. Then the genus $\gamma(\mathcal{E})$ of $\mathcal{E}$ satisfies*

$$\gamma(\mathcal{E}) = \lim_{r \to \infty} \frac{g(E_r)}{[E_r : E_0]} \leq \frac{q(q+2)}{2(q-1)}.$$

Proof. Let $\Phi := V(\mathcal{F}/F_0) \backslash \{(x_0 = 0), (x_0 = \infty)\}$. Using Proposition 4.3, Proposition 4.4 and Proposition 4.6, we see that the degree of the different of E_r/E_0 satisfies

$$\begin{aligned} \deg \mathrm{Diff}\ (E_r/E_0) &= \sum_{P \in \mathbb{P}(E_0)} \sum_{\substack{Q \in \mathbb{P}(E_r) \\ Q|P}} d(Q|P) = \sum_{P \in V(\mathcal{E}/E_0)} \sum_{\substack{Q \in \mathbb{P}(E_r) \\ Q|P}} d(Q|P) \\ &= \sum_{\substack{Q \in \mathbb{P}(E_r) \\ Q|(x_0=0)}} d(Q|P) + \sum_{\substack{Q \in \mathbb{P}(E_r) \\ Q|(x_0=\infty)}} d(Q|P) + \sum_{P \in \Phi} \sum_{\substack{Q \in \mathbb{P}(E_r) \\ Q|P}} d(Q|P) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{\substack{Q\in\mathbb{P}(E_r)\\ Q|(x_0=0)}} 2(e(Q|P)-1) + \sum_{\substack{Q\in\mathbb{P}(E_r)\\ Q|(x_0=\infty)}} \frac{q}{q-1}e(Q|P) + \sum_{P\in\Phi}\sum_{\substack{Q\in\mathbb{P}(E_r)\\ Q|P}} \frac{q}{q-1}e(Q|P)\\
&\le 2\sum_{\substack{Q\in\mathbb{P}(E_r)\\ Q|(x_0=0)}} e(Q|P) + \frac{q}{q-1}\sum_{\substack{Q\in\mathbb{P}(E_r)\\ Q|(x_0=\infty)}} e(Q|P) + \sum_{P\in\Phi}\frac{q}{q-1}\sum_{\substack{Q\in\mathbb{P}(E_r)\\ Q|P}} e(Q|P)\\
&= 2\cdot[E_r:E_0] + \frac{q}{q-1}[E_r:E_0] + \frac{q}{q-1}|\Phi|\cdot[E_r:E_0]\\
&= \frac{q^2+4q-2}{q-1}[E_r:E_0]
\end{aligned}
$$

Using Hurwitz genus formula, we get

$$2g(E_r)-2 = -2[E_r:E_0] + \deg \mathrm{Diff}(E_r/E_0) \le \frac{q^2+2q}{q-1}[E_r:E_0].$$

Therefore,

$$\lim_{r\to\infty}\frac{g(E_r)}{[E_r:E_0]} \le \frac{q(q+2)}{2(q-1)}.$$

□

Theorem 4.8. *Let $\mathcal{F}/\mathbb{F}_\ell$, with $\ell = q^3$ be the BGS tower and let $\mathcal{E} = (E_0, E_1, E_2, \ldots)$ be its Galois closure. Then $\mathcal{E}$ is a tower over $\mathbb{F}_\ell$ and its limit $\lambda(\mathcal{E})$ satisfies*

$$\lambda(\mathcal{E}) = \lim_{r\to\infty}\frac{N(E_r)}{g(E_r)} \ge \frac{2(q^2-1)}{q+2}.$$

Proof. Using Proposition 4.2 and Theorem 4.8, we obtain

$$\lambda(\mathcal{E}) = \frac{\nu(\mathcal{E})}{\gamma(\mathcal{E})} \ge \frac{2(q^2-1)}{q+2}.$$

□

Remark 4.9. In [2, Sec. 5], as a variation of the BGS tower, a new tower $\mathcal{B}$ is given. This tower $\mathcal{B}$ consists of alternating Kummer and Artin-Schreier extensions and contains the BGS tower as a subtower. It is shown, that the limit $\lambda(\mathcal{B})$ of this new tower satisfies

$$\lambda(\mathcal{B}) \ge \frac{2(q^2-1)}{q+2}.$$

It can be seen easily, that the tower $\mathcal{B}$ is a subtower of the Galois tower $\mathcal{E}$ constructed above. Hence the result about the limit of the tower $\mathcal{B}$ follows directly from Theorem 4.8.

5 The key lemma

We have seen above that the main difficulty in computing the genus of a tower is to resolve the ramification behaviour in composita, where the place is wildly ramified in both directions, since in this case Abhyankar's Lemma cannot be applied. The "key lemma" is a very useful tool in such situations. In the case of function fields, a proof of this lemma was given in [4]. Below, we give a proof of this result using the theory of higher ramification groups, which is applicable in a more general setting. For a more detailed exposition of the theory of higher ramification groups, we refer to [16].

Let F be a field, and let $v : F \to \mathbb{Z} \cup \{\infty\}$ be a discrete valuation of F with value group $\mathbb{Z}$. Let $\mathcal{O}$ and P denote the corresponding valuation ring and place of F; i.e.,

$$\mathcal{O} = \{a \in F | v(a) \geq 0\} \qquad \text{and} \qquad P = \{a \in F | v(a) > 0\}.$$

We will always assume that the residue class field $F_P := \mathcal{O}/P$ is perfect, and

$$\operatorname{char} F_P = p > 0.$$

We consider a Galois extension E/F whose Galois group $G = \operatorname{Gal}(E/F)$ is elementary-abelian of order p^2. Let Q be a place of E lying above P and denote by $G_i = G_i(Q|P)$ the i-th ramification group of $Q|P$, $i = 0, 1, 2 \ldots$.

Proposition 5.1. *Suppose that for some $s \geq 1$,*

$$G = G_0 = G_1 = \ldots = G_s \supsetneq G_{s+1} = \{id\}.$$

Let E' be an intermediate field of E/F with $[E' : F] = p$ and let P' be the restriction of Q to E'.

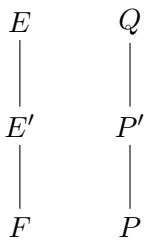

Figure 5.1:

Then $e(Q|P') = e(P'|P) = p$, and the different exponents are as follows:

$$d(Q|P) = (s+1)(p^2-1), \text{ and}$$

$$d(Q|P') = d(P'|P) = (s+1)(p-1).$$

Proof. By Hilbert's Different Formula (see [20, Ch. III.8]),

$$d(Q|P) = \sum_{i=0}^{\infty}(\operatorname{ord} G_i - 1) = (s+1)(p^2-1).$$

Now let $U := \mathrm{Gal}(E/E')$ and let $U_i = U_i(Q|P')$ denote the higher ramification groups of $Q|P'$. Then

$$U_i = U \cap G_i \text{ for all } i \geq 0,$$

hence

$$U_0 = U_1 = \cdots = U_s \supsetneqq U_{s+1} = \{id\}.$$

It follows that

$$d(Q|P') = (s+1)(p-1).$$

By transitivity of different exponents,

$$d(Q|P) = d(Q|P') + p \cdot d(P'|P),$$

hence

$$(s+1)(p^2-1) = (s+1)(p-1) + p \cdot d(P'|P).$$

So

$$d(P'|P) = \frac{1}{p}(s+1)(p^2-p) = (s+1)(p-1).$$

□

Proposition 5.2. *Suppose that for some $t > s \geq 1$,*

$$G = G_0 = \ldots = G_s \supsetneqq G_{s+1} = \ldots = G_t \supsetneqq G_{t+1} = \{id\}.$$

Let $U := G_{s+1}$, and denote by $H \leq G$ another subgroup of G of order p. Let $E' := E^U$ and $E_0 := E^H$, and let $P' := Q|_{E'}$ and $P_0 = Q|_{E_0}$.

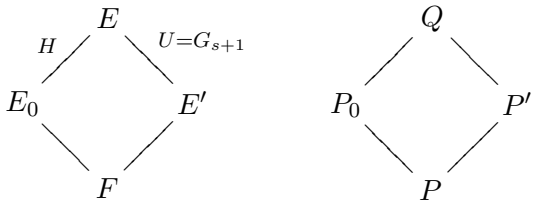

Figure 5.2:

Then the different exponents are as follows:

$$\begin{aligned}
d(Q|P) &= (s+1)(p^2-1) + (t-s)(p-1) \\
d(Q|P') &= (t+1)(p-1) \\
d(Q|P_0) &= (s+1)(p-1) \\
d(P'|P) &= (s+1)(p-1) \\
d(P_0|P) &= (s+1+\frac{t-s}{p})(p-1)
\end{aligned}$$

Proof. $d(Q|P)$ is clear from Hilbert's Different Formula.

Let $U_i = U_i(Q|P')$ resp. $H_i = H_i(Q|P_0)$ denote the ramification groups of $Q|P'$ resp. $Q|P_0$. Then

$$U_i = G_i \cap U = U \text{ for } i = 0, \dots, t, \text{ and } U_{t+1} = \{id\}.$$

Hence

$$d(Q|P') = (t+1)(p-1).$$

Also, $H_i = G_i \cap H = H$ for $i = 0, \dots, s$, and $H_i = \{id\}$ for $i \geq s+1$. Hence

$$d(Q|P_0) = (s+1)(p-1).$$

By transitivity,

$$d(Q|P) = d(Q|P') + p \cdot d(P'|P),$$

hence

$$(s+1)(p^2-1) + (t-s)(p-1) = (t+1)(p-1) + p \cdot d(P'|P).$$

So we obtain

$$d(P'|P) = \frac{1}{p}\Big((s+1)(p^2-1) - (s+1)(p-1)\Big) = (s+1)(p-1).$$

On the other hand,

$$d(Q|P) = d(Q|P_0) + p \cdot d(P_0|P),$$

hence

$$\begin{aligned} d(P_0|P) &= \frac{1}{p}\Big((s+1)(p^2-1) + (t-s)(p-1) - (s+1)(p-1)\Big) \\ &= \frac{1}{p}\Big((s+1)(p^2-p) + (t-s)(p-1)\Big) \\ &= (s+1)(p-1) + \frac{t-s}{p}(p-1). \end{aligned}$$

□

Proposition 5.2 is summarized in Figure 5.3)

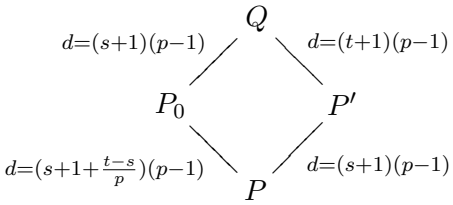

Figure 5.3:

Remark 5.3. Note that this gives a proof of the Hasse-Arf theorem in this situation; i.e., $s \equiv t \bmod p$.

We consider the situation as above; i.e., E/F is an elementary-abelian extension of degree p^2. Furthermore, P is a place of F and Q is a place of E lying above P. Assume that E_1, E_2 are intermediate fields of E/F with $[E_1 : F] = [E_2 : F] = p$ and $E_1 \neq E_2$. Denote by P_i the restriction of Q to E_i for $i = 1, 2$, and suppose that $e(P_1|P) = e(P_2|P) = p$.

Theorem 5.4. *Situation as above. Assume that*

$$d(P_1|P) = r_1(p-1) \qquad \text{and} \qquad d(P_2|P) = r_2(p-1)$$

with $r_1 \geq r_2$ (w.l.o.g.). Then the following holds:

(i) *If $r_1 > r_2$, then $Q|P$ is totally ramified and the different exponents of $Q|P_i$ are*

$$d(Q|P_1) = r_2(p-1),$$

$$d(Q|P_2) = (r_2 + p(r_1 - r_2))(p-1) = (r_1 + (p-1)(r_1 - r_2))(p-1).$$

(ii) *If $r_1 = r_2$, then there is an integer r with*

$$0 \leq r \leq r_1 \qquad \text{and} \qquad r \neq 1$$

such that

$$d(Q|P_1) = d(Q|P_2) = r(p-1).$$

Proof. (i) First note that in this case $Q|P$ is totally ramified (otherwise, $e(Q|P_1) = e(Q|P_2) = 1$ and we would get two different values for $d(Q|P) = d(P_i|P)$). So we are in the situation of Proposition 5.2, with $P_0 = P_1$ and $P' = P_2$. Using notation as in Proposition 5.2 we obtain

$$r_1 = s + 1 + \frac{t-s}{p} \qquad \text{and} \qquad r_2 = s + 1.$$

It follows from Proposition 5.2 that $d(Q|P_1) = d(P_2|P) = r_2(p-1)$, and

$$\frac{t-s}{p} = r_1 - r_2,$$

so

$$t = s + p(r_1 - r_2).$$

Therefore

$$t + 1 = s + 1 + p(r_1 - r_2) = r_2 + p(r_1 - r_2)$$

and

$$\begin{aligned} d(Q|P_2) &= (r_2 + p(r_1 - r_2))(p-1) \\ &= (r_1 + (p-1)(r_1 - r_2))(p-1). \end{aligned}$$

(ii) If $Q|P_i$ is unramified then we set $r = 0$. If $Q|P_i$ is ramified, we are either in the situation of Proposition 5.1 or of Proposition 5.2.

In Proposition 5.1 we get that $d(Q|P_1) = d(Q|P_2) = d(P_i|P)$, and we set $r := r_1 = r_2$.

In Proposition 5.2 we have that $r_1 = r_2 = s + 1 + \frac{t-s}{p}$, and we set $r := s + 1$; it is clear that $1 < r < r_1$. □

As an immediate corollary, we get

Corollary 5.5. *With the fields E, E_1, E_2 and F and the places Q, P_1, P_2 and P as above, assume that $d(P_i|P) = 2(e(P_i|P) - 1)$, for $i = 1, 2$. Then*

$$d(Q|P_i) = 2(e(Q|P_i) - 1), \text{ for } i = 1, 2.$$

Proof. If $P_1|P$ or $P_2|P$ is unramified, the statement is trivially true. Otherwise, we have $e(P_1|P) = e(P_2|P) = p$ and $d(P_1|P) = d(P_2|P) = 2(p-1)$. So by Theorem 5.4, (ii), either $Q|P_i$ is unramified, or $Q|P_i$ is totally ramified (i.e. $e(Q|P_i) = p$) and $d(Q|P_i) = 2(p-1)$, for $i = 1, 2$. In either case, $d(Q|P_i) = 2(e(Q|P_i) - 1)$ for $i = 1, 2$. □

As an easy consequence of the transitivity of different exponents in towers we get the following Lemma:

Lemma 5.6. *Let the field F and the place P of F be as above and let E be a finite separable extension of F. Let M be an intermediate field of E/F. Let Q be a place of E lying above P and let R be the restriction of Q to M. If $d(Q|R) = t(e(Q|R) - 1)$ and $d(R|P) = t(e(R|P) - 1)$ for some positive integer t, then $d(Q|P) = t(e(Q|P) - 1)$.*

Proof.

$$\begin{aligned} d(Q|P) &= d(R|P) \cdot e(Q|R) + d(Q|R) = t(e(R|P) - 1) \cdot e(Q|R) + t(e(Q|P) - 1) \\ &= t(e(Q|R) \cdot e(R|P) - 1) = t(e(Q|P) - 1). \end{aligned}$$

□

As a partial converse of Lemma 5.6, we have the following Lemma:

Lemma 5.7. *Situation as in Lemma 5.6. Suppose furthermore, that $[E : F] = p^n, n \geq 1$ and the extensions E/M and M/F are Galois. If $d(Q|P) = 2(e(Q|P) - 1)$, then*

$$d(Q|R) = 2(e(Q|R) - 1) \quad \text{and} \quad d(R|P) = 2(e(R|P) - 1).$$

Proof. See [5, Prop. 1.8]. □

Now we can easily prove the "key lemma":

Proposition 5.8. *Let the field F and the place P of F be as above. Let E_1 and E_2 be finite Galois p-extensions of F and let $E = E_1 \cdot E_2$ be the composite field of E_1 and E_2. Let Q be a place of E lying over P and let P_1 and P_2 be the restrictions of Q to E_1 and E_2, respectively. If the different exponents $d(P_i|P)$ satisfy*

$$d(P_i|P) = 2(e(P_i|P) - 1) \text{ for } i = 1, 2,$$

then $d(Q|P_i) = 2(e(Q|P_i) - 1)$ for $i = 1, 2$.

Proof. Let $G = \mathrm{Gal}(E_1/F)$ be the Galois group of the extension E_1/F. Since G is a p-group, we can find normal subgroups $G_0, G_1, G_2, \ldots G_r$ of G, s.t.

$$G = G_0 \supset G_1 \supset \ldots \supset G_r = \{id\}$$

and $(G_i : G_{i+1}) = p$ for $0 \leq i < r$. Taking the corresponding fixed fields, we obtain a refinement of the extension E_1/F into cyclic extensions of degree p, i.e. we have intermediate fields

$$F = T_0 \subset T_1 \subset \ldots \subset T_r = E_1,$$

where T_{i+1}/T_i, with $0 \leq i < r$, is a cyclic extension of degree p. Moreover, using Lemma 5.7, we see that $d(Q|_{T_{i+1}} \mid Q|_{T_i}) = 2(e(Q|_{T_{i+1}} \mid Q|_{T_i}) - 1)$ for $0 \leq i < r$.

Similarly, the extension E_2/F can be refined to a sequence of cyclic extensions of degree p, with $d = 2(e-1)$ in each step. Now repeated application of Corollary 5.5 and Lemma 5.6 gives the result. □

6 Asymptotic lower bounds for some classes of codes over cubic finite fields

It was shown in [21], that several classes of codes over finite fields with square cardinality, including the class of transitive codes and the class of self-dual codes, attain the Tsfasman–Vlăduţ–Zink bound. This was done by considering geometric Goppa codes obtained from a new Galois tower over a finite field with square cardinality. This Galois tower has only a single completely splitting place, but the tower is still asymptotically optimal. The code is constructed by evaluating functions at all places lying above this single completely splitting place. The transitive action of the Galois group on these places gives rise to a transitive automorphism group of the constructed codes.

In this section, we will consider the same problem over cubic finite fields. The starting point will be the BGS tower over cubic finite fields. Using the techniques from the previous sections, we will construct a Galois tower having the same limit as the BGS tower, but with less completely splitting places. This is accomplished by first collecting several completely splitting places above a small number of rational places of a subfield of the tower. Then the Galois closure of the BGS tower over this subfield is considered. The ideal case would be to be able to collect all rational places coming from completely splitting places over a single rational place of a subfield and still to get a Galois closure over this subfield with a good limit. This seems to be quite difficult. Hence we only go down to a subfield of degree q, which enables us to collect all rational places coming from completely splitting places over a total of $q+1$ places. We show that the Galois closure $\mathcal{E}'$ of the BGS tower over this subfields has the same limit as the BGS tower (see Theorem 6.4 below).

In analogy with the definition of r-quasi cyclic codes, we introduce the notion of r-quasi transitive codes (see Definition 6.9). Using the approach in [21], we obtain asymptotic lower bounds for this class of codes, over cubic finite fields. We also obtain an asymptotic lower bound for transitive isoorthogonal codes over cubic finite fields. The main tool is the tower $\mathcal{E}'$. This section closely follows [21].

6.1 Another Galois tower

Let $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ be the BGS tower over $\mathbb{F}_\ell$, as defined by Equation 2.1; i.e. $F_0 = \mathbb{F}_\ell(x_0)$ is the rational function field and $F_{i+1} = F_i(x_{i+1})$ where

$$x_{i+1}^q - x_{i+1}^{q-1} = 1 - x_i + \frac{1}{x_i^{q-1}} \quad \text{for } i \geq 0.$$

Let $w = x_0^q - x_0^{q-1}$. Then

$$\mathbb{F}_\ell(w) \subseteq \mathbb{F}_\ell(x_0) = F_0 \subseteq F_1 \subseteq \ldots.$$

The place $(w = \infty)$ of $\mathbb{F}_\ell(w)$ is totally ramified in the extension $\mathbb{F}_\ell(x_0)/\mathbb{F}_\ell(w)$ and $[\mathbb{F}_\ell(x_0) : \mathbb{F}_\ell(w)] = q$.

Consider the tower

$$\mathcal{F}' = (\mathbb{F}_\ell(w), \mathbb{F}_\ell(x_0) = F_0, F_1, \ldots),$$

and let $\mathcal{E}' = (\mathbb{F}_\ell(w), E_0, E_1, E_2, \ldots)$ be the Galois closure of $\mathcal{F}'$ over $\mathbb{F}_\ell(w)$; i.e., E_i is the Galois closure of the extension $F_i/\mathbb{F}_\ell(w)$, for $i = 0, 1, 2, \ldots$.

Let $\Phi \supseteq \mathbb{F}_\ell(w)$ be a fixed algebraically closed field. Let $r \geq 0$. Then we obtain E_r as

$$E_r = \sigma_1(F_r)\sigma_2(F_r)\cdots\sigma_s(F_r),$$

where $\sigma_1, \sigma_2 \ldots, \sigma_s$ are the embeddings of F_r into Φ over $\mathbb{F}_\ell(w)$

As defined in Section 2.3, let $S = \{\gamma \in \bar{\mathbb{F}}_\ell \mid \varphi(\gamma) = 0\}$. From the results in Section 2.3 we see that $S \subseteq \mathbb{F}_\ell$ and the places $(w = \alpha)$ of $\mathbb{F}_\ell(w)$ with $\alpha \in S$ split completely in the tower $\mathcal{F}'$. Hence, by Proposition 4.1, it follows $\mathcal{E}'$ is also a tower over $\mathbb{F}_\ell$. Furthermore we see that $Z(\mathcal{E}'/\mathbb{F}_\ell(w)) = Z(\mathcal{F}'/\mathbb{F}_\ell(w)) \supseteq \{(w = \alpha) \in \mathbb{P}(\mathbb{F}_\ell(w)) \mid \alpha \in S\}$ and $V(\mathcal{E}'/\mathbb{F}_\ell(w)) = V(\mathcal{F}'/\mathbb{F}_\ell(w))$. We immediately get the following corollary:

Corollary 6.1. *The splitting rate $\nu(\mathcal{E}')$ of the tower $\mathcal{E}'$ satisfies*

$$\nu(\mathcal{E}') = \lim_{i\to\infty} \frac{N(E_i)}{[E_i : \mathbb{F}_\ell(w)]} \geq |Z(\mathcal{E}'/\mathbb{F}_\ell(w))| \geq |S| = q + 1.$$

Next we want to estimate the genus of E_i for $i \geq 0$. We consider, as usual, the same tower over the algebraic closure $\bar{\mathbb{F}}_\ell$ of $\mathbb{F}_\ell$. let $R := \{\alpha \in \bar{\mathbb{F}}_\ell \mid \alpha^q - \alpha^{q-1} = 1\}$. The ramification in the extension $\bar{\mathbb{F}}_\ell(x_0)/\bar{\mathbb{F}}_\ell(w)$ can be easily computed (see Figure 6.1):

- The place $(w = \infty)$ of $\bar{\mathbb{F}}_\ell(w)$ is totally ramified in the extension $\bar{\mathbb{F}}_\ell(x_0)/\bar{\mathbb{F}}_\ell(w)$, the place of $\bar{\mathbb{F}}_\ell(x_0)$ lying over $(w = \infty)$ is the pole of x_0 in $\bar{\mathbb{F}}_\ell(x_0)$. We have

$$e((x_0 = \infty)|(w = \infty)) = q \text{ and } d((x_0 = \infty)|(w = \infty)) = q.$$

- There are two places of $\bar{\mathbb{F}}_\ell(x_0)$ extending the place $(w = 0)$ of $\bar{\mathbb{F}}_\ell(w)$. One is the zero of x_0 in $\bar{\mathbb{F}}_\ell(x_0)$ and the other one is the zero of $x_0 - 1$ in $\bar{\mathbb{F}}_\ell(x_0)$. The ramification indices are given as

$$e((x_0 = 0)|(w = 0)) = q - 1 \text{ and } e((x_0 = 1)|(w = 0)) = 1.$$

- All other places of $\bar{\mathbb{F}}_\ell(w)$ are unramified in the extension $\bar{\mathbb{F}}_\ell(x_0)/\bar{\mathbb{F}}_\ell(w)$.

- The places of $\bar{\mathbb{F}}_\ell(x_0)$ lying over the place $(w = 1)$ of $\bar{\mathbb{F}}_\ell(w)$ are the places $(x_0 = \alpha)$, with $\alpha \in R$.

Combining this with Lemma 2.4, we see that the ramification locus of $\mathcal{F}'$ over $\bar{\mathbb{F}}_\ell(w)$ is given as $V(\mathcal{F}'/\bar{\mathbb{F}}_\ell(w)) = \{(w = 0), (w = \infty), (w = 1)\}$, and by Proposition 4.1, we obtain

$$V(\mathcal{E}'/\bar{\mathbb{F}}_\ell(w)) = V(\mathcal{F}'/\bar{\mathbb{F}}_\ell(w)) = \{(w = 0), (w = \infty), (w = 1)\}.$$

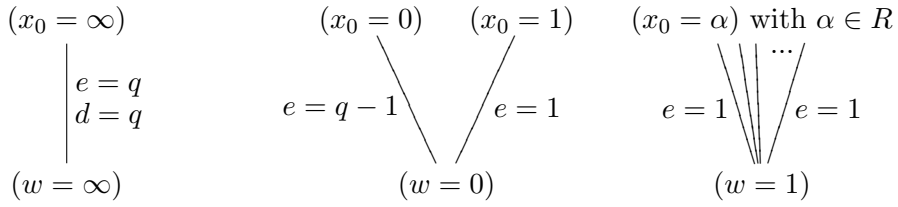

Figure 6.1:

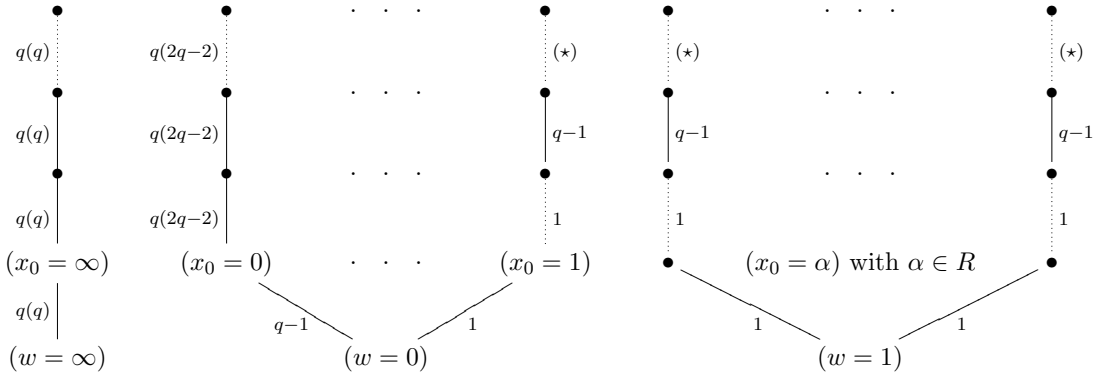

Figure 6.2:

Combining the information about the ramification in the extension $\bar{\mathbb{F}}_\ell(x_0)/\bar{\mathbb{F}}_\ell(w)$ with the results about the ramification behaviour in the BGS tower from Section 2, we see that the ramification in the tower $\mathcal{F}'$ is as depicted in Figure 6.2, where a dotted segment indicates that this segment might be repeated several times.

Remark 6.2. Note that the place $(w = \infty)$ of $\bar{\mathbb{F}}_\ell(w)$ is totally ramified in each step of the tower $\mathcal{F}'$. This will be used in the sequel.

Let $r \geq 0$, let Q be a place of E_r and let $P = Q|_{\bar{\mathbb{F}}_\ell(w)}$. Let $P' = Q|_{F_r}$. Suppose that $P = (w = 1)$. Then either P' is unramified over $\bar{\mathbb{F}}_\ell(w)$, or for some index t, with $1 \leq t \leq r$, we have:

- The restriction of P' to F_{t-1} is unramified over $\bar{\mathbb{F}}_\ell(w)$.
- The restriction of P' to F_t is tamely ramified over F_{t-1}, with ramification index $q - 1$.
- For $t < i \leq r$, the restriction of Q to F_i has property $(\star)$ for the extension F_i/F_{i-1}.

If $P = (w = 0)$, then the ramification behaviour of the place P' over P is also of the form described above (first tame ramification with ramification index $q - 1$, then extensions, where the restriction of P' has property $(\star)$).

So in either case (if $P = (w = 1)$ or $P = (w = 0)$) we can apply exactly the same reasoning as in Proposition 4.6, to conclude that

$$d(Q|P) \leq \frac{q}{q-1} e(Q|P).$$

Now, suppose that $P = (w = \infty)$. By lifting everything by $\bar{\mathbb{F}}_\ell(x_{-1})$, where

$$1 - x_{-1} + \frac{1}{x_{-1}^{q-1}} = w = x_0^q - x_0^{q-1}$$

we can apply exactly the same reasoning as in Proposition 4.4 to conclude that

$$d(Q|P) \leq \frac{q}{q-1} e(Q|P)$$

(see Figure 6.3).

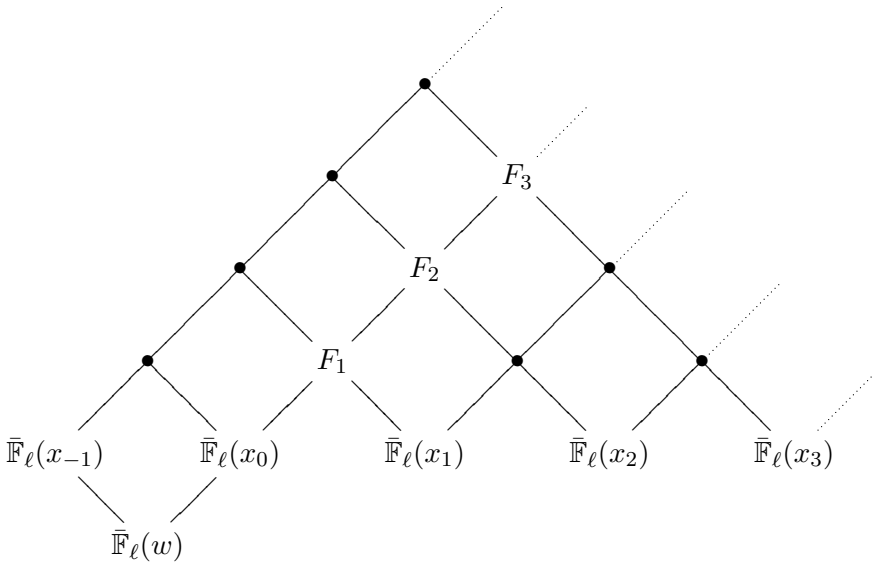

Figure 6.3:

Theorem 6.3. *The genus $\gamma(\mathcal{E}')$ of $\mathcal{E}'$ satisfies*

$$\gamma(\mathcal{E}') = \lim_{r\to\infty} \frac{g(E_r)}{[E_r : \bar{\mathbb{F}}_\ell(w)]} \leq \frac{q+2}{2(q-1)}.$$

Proof. We have seen above that for all $Q \in \mathbb{P}(E_r)$, such that $P = Q \cap \bar{\mathbb{F}}_\ell(w) \in V(\mathcal{E}'/\bar{\mathbb{F}}_\ell(w))$ we have

$$d(Q|P) \leq \frac{q}{q-1} e(Q|P).$$

So the degree of the different of E_r/E_0 satisfies

$$\deg \mathrm{Diff}\ (E_r/\bar{\mathbb{F}}_\ell(w)) = \sum_{P\in\mathbb{P}(\bar{\mathbb{F}}_\ell(w))} \sum_{\substack{Q\in\mathbb{P}(E_r)\\ Q|P}} d(Q|P) = \sum_{P\in V(\mathcal{E}'/\bar{\mathbb{F}}_\ell(w))} \sum_{\substack{Q\in\mathbb{P}(E_r)\\ Q|P}} d(Q|P)$$

$$\leq \sum_{P\in V(\mathcal{E}'/\bar{\mathbb{F}}_\ell(w))} \sum_{\substack{Q\in\mathbb{P}(E_r)\\ Q|P}} \frac{q}{q-1} e(Q|P) = \frac{q}{q-1} \sum_{P\in V(\mathcal{E}'/\bar{\mathbb{F}}_\ell(w))} \sum_{\substack{Q\in\mathbb{P}(E_r)\\ Q|P}} e(Q|P)$$

$$= \frac{q}{q-1} \cdot |V(\mathcal{E}'/\bar{\mathbb{F}}_\ell(w))| \cdot [E_r : \bar{\mathbb{F}}_\ell(w)] = \frac{3q}{q-1}[E_r : \bar{\mathbb{F}}_\ell(w)]$$

Using Hurwitz genus formula, we get

$$2g(E_r) - 2 = -2[E_r : E_0] + \deg \mathrm{Diff}(E_r/E_0) \leq \frac{q+2}{q-1}[E_r : E_0].$$

Therefore,

$$\lim_{r\to\infty} \frac{g(E_r)}{[E_r : E_0]} \leq \frac{q+2}{2(q-1)}.$$

□

Theorem 6.4. *The limit $\lambda(\mathcal{E}')$ of the tower $\mathcal{E}'$ satisfies*

$$\lambda(\mathcal{E}') = \lim_{r\to\infty} \frac{N(E_r)}{g(E_r)} \geq \frac{2(q^2-1)}{q+2}.$$

Proof. Using Corollary 6.1 and Theorem 6.3, we obtain

$$\lambda(\mathcal{E}') = \frac{\nu(\mathcal{E}')}{\gamma(\mathcal{E}')} \geq \frac{2(q^2-1)}{q+2}.$$

□

Remark 6.5. While constructing the tower above, we first went down to a subfield $\mathbb{F}_\ell(w)$, in order to collect all rational places coming from completely splitting places over a total of $q+1$ places. Letting furthermore

$$z = w^{q+1} - w + 1,$$

it is even possible to collect all such places over a single place, namely the place $(z = 0)$ of $\mathbb{F}_\ell(z)$. However in this case, estimating the genus of the Galois closure of the tower over $\mathbb{F}_\ell(z)$ seems to be more difficult. The techniques used above do not suffice.

6.2 Finite permutation groups and quasi transitive codes

Let us start by recalling some basic facts about group actions and finite permutation groups. We restrict to the finite case, since this is the case needed in the sequel. For a more detailed exposition, see [10, 14, 23].

Let G be a group acting on a finite set A. We will denote the permutation of A associated to the element $x \in G$ by π_x and for $a \in A$ we write $a^x := \pi_x(a)$.

For $a \in A$, we denote by G_a the stabilizer (isotropy group) of a in G and we denote the orbit of a under G by a^G. It can be shown that for $a \in A$, we have

$$|a^G| = (G : G_a) \tag{6.1}$$

The group G is said to act transitively on the set A, if there is just one orbit under the action of G on A; i.e., if for all $a_1, a_2 \in A$ there is a $g \in G$, such that $a_1^g = a_2$. The action of G on A is said to be half-transitive or $\frac{1}{2}$-fold transitive, if the orbits of the action of G on A all have equal length. By Equation 6.1, it is easy to see that G acts half-transitively on A, if and only if $|G_a|$ is the same for all $a \in A$. If $G_a = \{id\}$ for all $a \in A$, then the action of G is said to be semiregular. Note that by Equation 6.1, an action G is semiregular if and only if G acts half-transitively on A and $|a^G| = |G|$ for some (and hence for all) $a \in G$.

Lemma 6.6. *Let G be a finite group with a semiregular action on a finite set A. Suppose that the action of G on A has r distinct orbits and let $m = |G|$. Then there exists an enumeration*

$$A := (a_{1,1}, a_{1,2}, \ldots, a_{1,m},\ a_{2,1}, a_{2,2}, \ldots, a_{2,m},\ \ldots,\ a_{r,1}, a_{r,2}, \ldots, a_{r,m}),$$

of the elements of A with the following property:

For all integers i, j with $1 \leq i, j \leq m$, there exists an element $\sigma \in S_m$ and an element $g \in G$, such that $\sigma(i) = j$ and

$$a_{h,k}^g = a_{h,\sigma(k)},$$

for all $1 \leq h \leq r$, $1 \leq k \leq m$. In particular,

$$a_{1,i}^g = a_{1,j}, \quad a_{2,i}^g = a_{2,j}, \quad \ldots, \quad a_{m,i}^g = a_{m,j}.$$

Proof. For an element $a \in A$, consider the map $\rho_a : G \to a^G$ defined by $\rho_a(g) = a^g$ for $g \in G$. Obviously, this map is surjective. Since the action of G is semiregular, ρ_a will be injective, and hence a bijection from G to a^G. Let $G = \{g_1 = id, g_2, \ldots, g_m\}$, and let $a_1, a_2, \ldots, a_r$ be elements from distinct orbits of G. For $1 \leq h \leq r$, $1 \leq k \leq m$, let $a_{h,k} = \rho_{a_h}(g_k) = a_h^{g_k}$. Letting $g = g_i^{-1} g_j$ we see that $a_{h,k}^g = (a_h^{g_k})^{g_i^{-1} g_j} = a_h^{g_k g_i^{-1} g_j}$ and the above statements follow easily. Note that in the proof it is crucial that the action of the group is semiregular. □

Next, let us recall some basic definitions from coding theory and define the notion of a quasi transitive code. For details about quasi cyclic codes, we refer to [11]. For

details about codes in general, see for instance [12, 15]. Let $\mathbb{F}_\ell$ be the finite field with ℓ elements. For a linear code $\mathcal{C}$ over $\mathbb{F}_\ell$, we will denote by $n(\mathcal{C}), k(\mathcal{C})$ and $d(\mathcal{C})$ the length, the dimension and the minimum distance of the code, respectively.

Definition 6.7. A code $\mathcal{C}$ over $\mathbb{F}_\ell$ is said to be transitive, if its automorphism group $\mathrm{Aut}(\mathcal{C})$ is a transitive subgroup of S_n; i.e. if for all integers i, j with $1 \leq i, j \leq n$, there exists a permutation $\pi \in \mathrm{Aut}(\mathcal{C})$, such that $\pi(i) = j$.

Definition 6.8. Let r and m be positive integers. Let $\mathcal{C}$ be a (linear) code of length $n := r \cdot m$ over $\mathbb{F}_\ell$. Let T denote the standard cyclic shift operator on $\mathbb{F}_\ell^n$. The code $\mathcal{C}$ is said to be a *r-quasi cyclic code* or a *quasi-cyclic code of index r*, if it is invariant under T^r.

Note that a quasi-cyclic code of index 1 is a cyclic code. Obviously, every r-quasi cyclic code of length $n = r \cdot m$ over $\mathbb{F}_\ell$ is permutation equivalent to a code, which is invariant under the operator V_r on $\mathbb{F}_\ell^n$, which maps

$$(c_{1,1}, c_{1,2}, \ldots, c_{1,m},\ c_{2,1}, c_{2,2}, \ldots, c_{2,m},\ \ldots,\ c_{r,1}, c_{r,2}, \ldots, c_{r,m})$$

to

$$(c_{1,m}, c_{1,1}, \ldots, c_{1,m-1},\ c_{2,m}, c_{2,1}, \ldots, c_{2,m-1},\ \ldots,\ c_{r,m}, c_{r,1}, \ldots, c_{r,m-1}).$$

As a generalization of quasi-cyclic codes, we make the following definition:

Definition 6.9. Let r and m be positive integers. Let $\mathcal{C}$ be a (linear) code of length $n := r \cdot m$ over $\mathbb{F}_\ell$. The code $\mathcal{C}$ is said to be a *r-quasi transitive code* or a *quasi-transitive code of index r*, if there exists a transitive subgroup U of S_m, such that for all $\sigma \in U$, the code $\mathcal{C}$ is invariant under the operator V_σ, which maps

$$(c_{1,1}, c_{1,2}, \ldots, c_{1,m},\ c_{2,1}, c_{2,2}, \ldots, c_{2,m},\ \ldots,\ c_{r,1}, c_{r,2}, \ldots, c_{r,m})$$

to

$$(c_{1,\sigma(1)}, c_{1,\sigma(2)}, \ldots, c_{1,\sigma(m)},\ c_{2,\sigma(1)}, c_{2,\sigma(2)}, \ldots, c_{2,\sigma(m)},\ \ldots,\ c_{r,\sigma(1)}, c_{r,\sigma(2)}, \ldots, c_{r,\sigma(m)}).$$

In other words, if $\mathcal{C}$ is a r-quasi transitive code of length $r \cdot m$, then for all integers i, j, with $1 \leq i, j \leq m$, there exists a permutation $\pi \in \mathrm{Aut}(\mathcal{C})$, such that $\pi(i + km) = j + km$ for all $0 \leq k \leq r - 1$ and $\pi(t + km) = \pi(t) + km$ for all $1 \leq t \leq m$, $0 \leq k \leq r - 1$.

6.3 Asymptotic lower bounds for quasi transitive codes

Next, we use the tower $\mathcal{E}'$ considered above to construct arbitrarily long quasi transitive codes over cubic finite fields with good error correcting parameters. Hence we obtain asymptotic lower bounds for the class of quasi transitive codes. We closely follow the approach in [21].

Theorem 6.10. *Let $\ell = q^3$. Let $t \in \{1, 2, \ldots, q+1\}$ and let $R, \delta \geq 0$ with*

$$R = 1 - \delta - \frac{1}{t}\frac{q+2}{2(q-1)}.$$

Then there exists a sequence $(\mathcal{C}_j)_{j\geq 0}$ of linear codes $\mathcal{C}_j$ over $\mathbb{F}_\ell$ such that

1. *$\mathcal{C}_j$ is a t-quasi transitive code for all $j \geq 0$,*
2. *$n(\mathcal{C}_j) \to \infty$ as $j \to \infty$,*
3. *$\lim_{j\to\infty} k(\mathcal{C}_j)/n(\mathcal{C}_j) \geq R$ and $\lim_{j\to\infty} d(\mathcal{C}_j)/n(\mathcal{C}_j) \geq \delta$.*

Proof. Let $\epsilon > 0$. The proof proceeds by constructing arbitrary long t-quasi transitive codes $\mathcal{C}$ over $\mathbb{F}_\ell$, such that $k(\mathcal{C})/n(\mathcal{C}) \geq R - \epsilon$ and $d(\mathcal{C})/n(\mathcal{C}) \geq \delta$. Consider the tower $\mathcal{E}' = (\mathbb{F}_\ell(w), E_0, E_1, E_2, \ldots)$ constructed above. Choose an integer n large enough, so that

$$\frac{1}{t \cdot l^{n+1}} < \epsilon. \tag{6.2}$$

Let $N := [E_n : \mathbb{F}_\ell(w)]$ and, as above, let $S = \{\gamma \in \bar{\mathbb{F}}_\ell \mid \gamma^{q+1} - \gamma + 1 = 0\}$. We have seen above, that the places $(w = \alpha)$ with $\alpha \in S$ split completely in the tower E'. Let U be a subset of S with $|U| = t$. Define the following divisors of E_n:

$$D := \sum_{\substack{P\in\mathbb{P}(E_n)\\ w(P)\in U}} P \quad \text{and} \quad G_0 := \sum_{\substack{Q\in\mathbb{P}(E_n)\\ w(Q)=\infty}} Q.$$

Then $\deg D = t \cdot N$ and by Remark 6.2

$$\deg G_0 \leq \frac{[E_n : \mathbb{F}_\ell(w)]}{[F_n : \mathbb{F}_\ell(w)]} \leq \frac{N}{l^{n+1}}.$$

Using Inequality 6.2, we see that $(\deg G_0)/(t \cdot N) < \epsilon$. Choose $r \geq 0$, such that

$$1 - \delta \geq r \cdot \frac{\deg G_0}{t \cdot N} > 1 - \delta - \epsilon. \tag{6.3}$$

Consider the geometric Goppa code $\mathcal{C} := \mathcal{C}_\mathcal{L}(D, rG_0)$. Then $n(\mathcal{C}) = t \cdot N$ and by standard estimates for the parameters of geometric Goppa codes (see [20, Ch. II.2]), Inequality 6.3 and Theorem 6.3, we obtain

$$\frac{k(\mathcal{C})}{n(\mathcal{C})} = \frac{k(\mathcal{C})}{t \cdot N} \geq \frac{r \cdot \deg G_0}{t \cdot N} + \frac{1}{t \cdot N} - \frac{1}{t}\frac{g(E_N)}{N} > 1 - \delta - \epsilon - \frac{1}{t}\frac{q+2}{2(q-1)} = R - \epsilon$$

and

$$\frac{d(\mathcal{C})}{n(\mathcal{C})} = \frac{d(\mathcal{C})}{t \cdot N} \geq 1 - \frac{r \cdot \deg G_0}{t \cdot N} \geq \delta.$$

The Galois group $\Gamma := \mathrm{Gal}(E_n/\mathbb{F}_\ell(w)$ acts on the places in the support of D. Moreover, for a place P in the support of D, the stabilizer Γ_P of P in Γ is just the decomposition

group of P over $P \cap \mathbb{F}_\ell(w)$. Since the place $P \cap \mathbb{F}_\ell(w)$ splits completely in the extension $E_n/\mathbb{F}_\ell(w)$, we have $\Gamma_P = \Gamma_{-1}(P \mid P \cap \mathbb{F}_\ell(w)) = \{id\}$. So the action of Γ on $\operatorname{supp} D$ is semiregular and each orbit has length $|\Gamma|$. So this action has a total of $\deg D/|\Gamma| = (Nt)/N = t$ orbits.

Since the divisor rG_0 is invariant under the action of Γ, the semiregular action of Γ on $\operatorname{supp} D$ yields an action of Γ on $\mathcal{C} = \mathcal{C}_\mathcal{L}(D, rG_0)$. So by using Lemma 6.6, we see that the code $\mathcal{C}$ is (permutation equivalent to) a t-quasi transitive code. □

For $q = 7, \ell = 7^3$ the graph of the Gilbert-Varshamov bound and the bounds obtained above for various values of t is given in Figure 6.4.

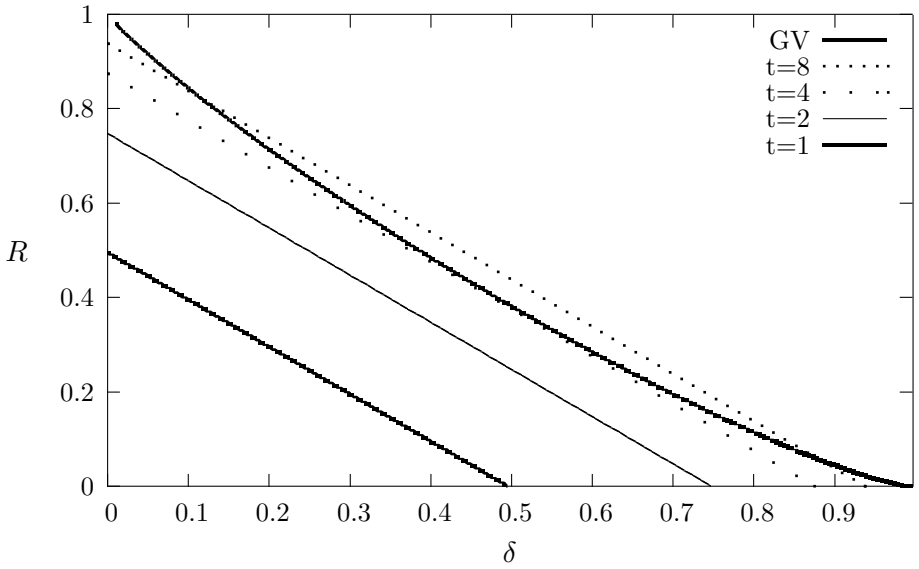

Figure 6.4: $q = 7$

Note that 1-quasi transitive codes are just transitive codes. By letting $t = 1$ in the above theorem, we immediately get the following corollary:

Corollary 6.11. *Let $\ell = q^3$. Let $R, \delta \geq 0$ with $R = 1 - \delta - \frac{q+2}{2(q-1)}$. Then there exists a sequence $(\mathcal{C}_j)_{j \geq 0}$ of linear codes $\mathcal{C}_j$ over $\mathbb{F}_\ell$ such that*

1. *$\mathcal{C}_j$ is a transitive code for all $j \geq 0$,*
2. *$n(\mathcal{C}_j) \to \infty$ as $j \to \infty$,*
3. *$\lim_{j\to\infty} k(\mathcal{C}_j)/n(\mathcal{C}_j) \geq R$ and $\lim_{j\to\infty} d(\mathcal{C}_j)/n(\mathcal{C}_j) \geq \delta$.*

6.4 An asymptotic lower bound for transitive isoorthogonal codes

In this section we will, following [21], develop asymptotic lower bounds for the class of transitive isoorthogonal codes over cubic finite fields. This will again be accomplished by use of the tower $\mathcal{E}'$ above.

Let us start by recalling some basic definitions from coding theory. For more details, we refer to [12, 15]. Let $\mathcal{C}$ be a linear code over $\mathbb{F}_\ell$ of length n. There is a canonical non-degenerate bilinear form on $\mathbb{F}_\ell^n \times \mathbb{F}_\ell^n$, defined by

$$< a, b >:= \sum_{i=1}^{n} a_i b_i$$

for $a = (a_1, a_2, \ldots, a_n)$ and $b = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_\ell^n$. The dual code $\mathcal{C}^\perp$ of the code $\mathcal{C}$ is defined as

$$\mathcal{C}^\perp := \{x \in \mathbb{F}_\ell^n | < x, c >= 0 \text{ for all } c \in \mathcal{C}\}.$$

The code $\mathcal{C}$ is called *self-dual*, if $\mathcal{C} = \mathcal{C}^\perp$. The code $\mathcal{C}$ is called *self-orthogonal*, if $\mathcal{C} \subseteq \mathcal{C}^\perp$. Let $a = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_\ell^n$ with $a_1, a_2, \ldots, a_n \neq 0$. We define

$$a \cdot \mathcal{C} := \{(a_1 \cdot c_1, a_2 \cdot c_2, \ldots, a_n \cdot c_n) | (c_1, c_2, \ldots, c_n) \in \mathcal{C}\} \subseteq \mathbb{F}_\ell^n.$$

The codes $\mathcal{C}$ and $a \cdot \mathcal{C}$ are said to be *equivalent*. Obviously, equivalent codes have the same parameters. The code $\mathcal{C}$ is called *isodual* if $\mathcal{C}$ is equivalent to its dual code $\mathcal{C}^\perp$. The code $\mathcal{C}$ is said to be *isoorthogonal* if $\mathcal{C}$ is equivalent to a subcode of $\mathcal{C}^\perp$.

In [19], sufficient conditions for self-duality and self-orthogonality of geometric Goppa codes are given. We will use these conditions and the tower $\mathcal{E}'$ considered above to obtain arbitrary long sequences of transitive isoorthogonal codes over the cubic finite field $\mathbb{F}_\ell$ with good error correcting parameters. First we recall some results from [19].

Theorem 6.12. *Let $F/\mathbb{F}_\ell$ be an algebraic function field over the finite field $\mathbb{F}_\ell$. Let $P_1, P_2, \ldots P_n$ be pairwise different rational places of $F/\mathbb{F}_\ell$. Put $D = P_1 + P_2 + \ldots + P_n$, and let G be a divisor of $F/\mathbb{F}_\ell$, such that $\operatorname{supp} G \cap \operatorname{supp} D = \varnothing$. Suppose there is a canonical divisor W, such that*

1. *$W + D \geq 2G$,*
2. *$v_{P_i}(W) = -1$, for $i = 1, 2, \ldots, n$.*

Then, the geometric Goppa code $\mathcal{C}_\mathcal{L}(D, G)$ is isoorthogonal; i.e., there exists an $a \in (\mathbb{F}_\ell \backslash \{0\})^n$ such that

$$a \cdot \mathcal{C}_\mathcal{L}(D, G) \subseteq \mathcal{C}_\mathcal{L}(D, G)^\perp.$$

The vector a can be given as follows: let η be a differential of F, such that $(\eta) = W$. Then

$$a = (\operatorname{res}_{P_1}\eta, \operatorname{res}_{P_2}\eta, \ldots, \operatorname{res}_{P_n}\eta),$$

where $\operatorname{res}_{P_i}\eta$ denotes the residue of the differential η at the place P_i.

Proof. See [19]. □

Now let $\ell = q^3$ and consider the the tower $\mathcal{E}'/\mathbb{F}_\ell$ constructed above. Recall, that the ramification locus of the tower is given as

$$V(\mathcal{E}'/\mathbb{F}_\ell(w)) = \{(w = 0), (w = \infty), (w = 1)\}.$$

For $n \geq 0$, let

$$A_0^{(n)} = \sum_{\substack{P \in \mathbb{P}(E_n) \\ P|(w=0)}} P, \quad A_\infty^{(n)} = \sum_{\substack{P \in \mathbb{P}(E_n) \\ P|(w=\infty)}} P \quad \text{and} \quad A_1^{(n)} = \sum_{\substack{P \in \mathbb{P}(E_n) \\ P|(w=1)}} P.$$

For $n \geq 0$, let $e_0^{(n)}, e_\infty^{(n)}$ and $e_1^{(n)}$ be integers, so that

$$\mathrm{Con}_{E_n/\mathbb{F}_\ell(w)}((w=0)) = e_0^{(n)} \cdot A_0^{(n)}, \quad \mathrm{Con}_{E_n/\mathbb{F}_\ell(w)}((w=\infty)) = e_\infty^{(n)} \cdot A_\infty^{(n)}$$

and

$$\mathrm{Con}_{E_n/\mathbb{F}_\ell(w)}((w=1)) = e_1^{(n)} \cdot A_1^{(n)}.$$

Similarly, for $n \geq 0$, let $d_0^{(n)}, d_\infty^{(n)}$ and $d_1^{(n)}$ be integers, so that

$$\mathrm{Diff}(E_n/\mathbb{F}_\ell(w)) = d_0^{(n)} \cdot A_0^{(n)} + d_\infty^{(n)} \cdot A_\infty^{(n)} + d_1^{(n)} \cdot A_1^{(n)}.$$

Theorem 6.13. *Let $\ell = q^3$ and let $0 \leq R \leq 1/2, \delta \geq 0$ with*

$$R = 1 - \delta - \frac{q+2}{2(q-1)}.$$

Then there exists a sequence $(\mathcal{C}_j)_{j \geq 0}$ of linear codes $\mathcal{C}_j$ over $\mathbb{F}_\ell$ such that

1. *$\mathcal{C}_j$ is a transitive isoorthogonal code for all $j \geq 0$,*
2. *$n(\mathcal{C}_j) \to \infty$ as $j \to \infty$,*
3. *$\lim_{j\to\infty} k(\mathcal{C}_j)/n(\mathcal{C}_j) \geq R$ and $\lim_{j\to\infty} d(\mathcal{C}_j)/n(\mathcal{C}_j) \geq \delta$.*

Proof. Let $S = \{\gamma \in \bar{\mathbb{F}}_\ell \mid \gamma^{q+1} - \gamma + 1 = 0\} \subseteq \mathbb{F}_\ell$. We have seen above, that the places $(w = \alpha)$ with $\alpha \in S$ split completely in the tower E'. Fix an element $\xi \in S$. Then the place $(w = \xi)$ of $\mathbb{F}_\ell(w)$ splits completely in the tower $\mathcal{E}'$. Define the following divisor of E_n:

$$D^{(n)} := \sum_{\substack{P \in \mathbb{P}(E_n) \\ P|(w=\xi)}} P.$$

Consider the differential

$$\eta := \frac{\mathrm{d}w}{w - \xi}.$$

The divisor of η in E_n is given by

$$\begin{aligned} W^{(n)} = (\eta) &= -(w-\xi)^{E_n} - 2(w)_\infty^{E_n} + \mathrm{Diff}(E_n/\mathbb{F}_\ell(w)) \\ &= e_\infty^{(n)} \cdot A_\infty^{(n)} - \sum_{\substack{P \in \mathbb{P}(E_n) \\ P|(w=\xi)}} P - 2e_\infty^{(n)} \cdot A_\infty^{(n)} + d_0^{(n)} \cdot A_0^{(n)} + d_\infty^{(n)} \cdot A_\infty^{(n)} + d_1^{(n)} \cdot A_1^{(n)} \\ &= d_0^{(n)} \cdot A_0^{(n)} + (e_\infty^{(n)} - 2e_\infty^{(n)} + d_\infty^{(n)}) \cdot A_\infty^{(n)} + d_1^{(n)} \cdot A_1^{(n)} - D^{(n)} \\ &= a_n A_0^{(n)} + b_n A_\infty^{(n)} + c_n A_1^{(n)} - D^{(n)}, \end{aligned}$$

where $a_n = d_0^{(n)}, b_n = e_\infty^{(n)} - 2 \cdot e_\infty^{(n)} + d_\infty^{(n)}$ and $c_n = d_1^{(n)}$. Note that $v_P(W^{(n)}) = -1$ for all $P \in \operatorname{supp} D^{(n)}$, and $W^{(n)} + D^{(n)} = a_n A_0^{(n)} + b_n A_\infty^{(n)} + c_n A_1^{(n)}$.

For integers a, b, c with $0 \le a \le a_n/2$, $0 \le b \le b_n/2$ and $0 \le c \le c_n/2$, consider the divisor

$$H_{a,b,c}^{(n)} = aA_0^{(n)} + bA_\infty^{(n)} + cA_1^{(n)},$$

and define the geometric Goppa code

$$\mathcal{C}_{a,b,c}^n := \mathcal{C}_\mathcal{L}(D^{(n)}, H_{a,b,c}^{(n)}).$$

We have

$$2H_{a,b,c} = 2aA_0^{(n)} + 2bA_\infty^{(n)} + 2cA_1^{(n)} \le a_n A_0^{(n)} + b_n A_\infty^{(n)} + c_n A_1^{(n)} = W^{(n)} + D^{(n)},$$

so by Theorem 6.12, we see that the code $C_{a,b,c}^n$ is isoorthogonal for all a, b, c with $0 \le a \le a_n/2$, $0 \le b \le b_n/2$ and $0 \le c \le c_n/2$. The Galois group of $E_n/\mathbb{F}_\ell(w)$ acts transitively on all places in the support of $D^{(n)}$, which consists just of all places of E_n lying over the place $(w = \xi)$ of $\mathbb{F}_\ell(w)$. Furthermore, the divisors $A_0^{(n)}, A_\infty^{(n)}$ and $A_1^{(n)}$ are invariant under the action of the Galois group of $E_n/\mathbb{F}_\ell(w)$. Therefore the code $C_{a,b,c}^n$ is transitive. Using the same argument as in the proof of Theorem 6.10, we see that such sequences of codes can be found. □

Remark 6.14. Let $\ell = q^3$. Let $t \in \{1, 2, \ldots, q+1\}$ and let $0 \le R \le 1/2, \delta \ge 0$ with

$$R = 1 - \delta - \frac{3 + t(q-1)}{2t(q-1)}.$$

Then one can show that there exists a sequence $(\mathcal{C}_j)_{j \ge 0}$ of t-quasi transitive isoorthogonal linear codes $\mathcal{C}_j$ over $\mathbb{F}_\ell$ with $n(\mathcal{C}_j) \to \infty$ as $j \to \infty$ such that $\lim_{j\to\infty} k(\mathcal{C}_j)/n(\mathcal{C}_j) \ge R$ and $\lim_{j\to\infty} d(\mathcal{C}_j)/n(\mathcal{C}_j) \ge \delta$.

Bibliography

[1] P. Beelen, A. Garcia, H. Stichtenoth, *Towards a classification of recursive towers of function fields over finite fields*, Finite Fields Appl. **12**, No. 1, 2006, 56-77.

[2] J. Bezerra, A. Garcia, H. Stichtenoth, *An explicit tower of function fields over cubic finite fields and Zink's lower bound*, J. Reine Angew. Math. **589**, 2005, 159-199.

[3] V. G. Drinfel'd, S. G. Vlăduţ, *The number of points of an algebraic curve*, Func. Anal. **17**, 1983, 53-54.

[4] A. Garcia, H. Stichtenoth, *Some Artin-Schreier towers are easy*, Mosc. Math. J. **5**, No. 4, 2005, 767-774.

[5] A. Garcia, H. Stichtenoth, *On the Galois closure of towers*, preprint 2005.

[6] A. Garcia, H. Stichtenoth, *On the asymptotic behaviour of some towers of functions fields over finite fields*, J. Number Theory **61**, No. 2, 1996, 248-273.

[7] A. Garcia, H. Stichtenoth, M. Thomas, *On towers and composita of towers of function fields over finite fields*, Finite Fields Appl. **3**, No. 3, 1997, 257-274.

[8] G. van der Geer, M. van der Vlugt, *An asymptotically good tower of curves over the field with eight elements*, Bull. London Math. Soc. **34**, No. 3, 2002, 291-300.

[9] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28**, 1981, 721-724.

[10] S. Lang, *Algebra, 3rd revised ed.*, Springer Verlag, New York, 2002.

[11] S. Ling, P. Solé, *On the algebraic structure of quasi-cyclic codes I: Finite Fields*, IEEE Trans. Inform. Theory **47**, No. 7, 2001, 2751-2760.

[12] Y. J. MacWilliams, N. J. A. Sloane, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam, 1977.

[13] Y. I. Manin, *What is the maximum number of points on a curve over* $\mathbb{F}_2$*?*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28**, 1981, 715-720.

[14] D. S. Passman, *Permutation Groups*, W.A. Benjamin, Inc., New York-Amsterdam, 1968.

[15] *Handbook of Coding Theory*, vol. I and II (eds. V. S. Pless, W. C. Huffmann), Elsevier, Amsterdam, 1998.

[16] J.-P. Serre, *Local Fields*, Springer Verlag, New York-Berlin, 1979.

[17] J.-P. Serre, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, C. R. Acad. Sci. Paris **296**, No. 9, 1983, 397-402.

[18] J.-P. Serre, *Rational points on curves over finite fields*, unpublished lecture notes by F. Q. Gouvêa, Harvard University, 1985.

[19] H. Stichtenoth, *Self-dual Goppa codes*, J. Pure Appl. Algebra **55**, No. 1-2, 1988, 199-211.

[20] H. Stichtenoth, *Algebraic function fields and codes*, Springer Verlag, Berlin, 1993.

[21] H. Stichtenoth, *Transitive and self-dual codes attaining the Tsfasman–Vlăduţ–Zink bound*, IEEE Trans. Inform. Theory **52**, No. 5, 2006, 2218-2224.

[22] M. A. Tsfasman, S. G. Vlăduţ, T. Zink, *Modular curves, Shimura curves, and Goppa codes, better than the Varshamov-Gilbert bound*, Math. Nachr. **109**, 1982, 21-28.

[23] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York-London, 1964.

[24] T. Zink, *Degeneration of Shimura surfaces and a problem in coding theory*, in Fundamentals of Computation Theory (L. Budach, ed.), Lecture Notes in Computer Science, Vol. **199**, Springer Verlag, Berlin, 1985, 503-511.